UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA: INGENIERÍA EN SISTEMAS

Tesis previa a la obtención del título de:
INGENIERO EN SISTEMAS

TEMA:
ANÁLISIS Y EMULACIÓN DE MULTIHOMING Y DE LA PUBLICACIÓN AL INTERNET DE SERVICIOS WEB, TRANSFERENCIA DE ARCHIVOS Y CORREO A TRAVÉS DE UNA RED IPv6

AUTOR:
FAUSTO RENE FLORES CALAHORRANO

DIRECTOR:
JORGE ENRÍQUE LÓPEZ LOGACHO

Quito, enero del 2014

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Yo Fausto Rene Flores Calahorrano autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

Fausto Rene Flores Calahorrano
CC 1712795986

DEDICATORIA

A:

Mis padres Enma Calahorrano y Fausto Flores, por ser mí guías y el ejemplo que sigo todos los días, porque siempre recibí su apoyo incondicional y buenos consejos.

Mis hermanas; Lorena y Anita, ya que gracias a su ejemplo, apoyo y ayuda pude tener un ambiente familiar lleno de buenos consejos.

AGRADECIMIENTO

Agradezco a la Universidad Politécnica Salesiana y a sus docentes que durante todo el transcurso de mi vida estudiantil, fueron quienes me encaminaron y guiaron hacia la profesionalización y culminación de la carrera, compartiendo su conocimiento y sobre todo su amistad y de manera especial al Ingeniero Jorge López por la paciencia y el aporte académico en la dirección de este trabajo.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El proyecto de trabajo de grado está encaminado al estudio y emulación de un entorno de red, en el cual un ISP publica su Sistema Autónomo y trabaja con OSPFv3 e IPv6, a través de BGP- Multihoming además de los servicios WEB, FTP y Correo Electrónico.

El trabajo se ha enfocado en una solución Multihomed que está orientada a los proveedores de servicio que presentan inconvenientes en la transmisión de datos, en el momento en que uno de sus enlaces WAN falla y como consecuencia la afectación del servicio para sus clientes.

Con la emulación se busca clarificar la teoría y crear escenario de pruebas apegado a la realidad, así como comprender el funcionamiento de los protocolos involucrados. Para el desarrollo del trabajo se siguieron los siguientes lineamientos:

1. Verificar las características que la red requiere en la transferencia de información.
2. Diseño de la topología física y lógica.
3. Esquema de direccionamiento IPv6.
4. Configuraciones en los equipos de acuerdo al modelo deseado.
5. Aplicar las configuraciones en la emulación del entorno de red.

El entorno de red se comunica a través IPv6 y cuenta con enlaces WAN configurados de respaldo de manera que trabajan de forma automática. De la misma manera los servicios HTTP, FTP y SMTP hacen uso del entorno de red por medio de IPv6.

El proyecto se ha enfocado en el análisis y configuración bajo un ambiente emulado con VMWare y GNS3 de los protocolos Open Shortest Path First versión 3 (OSPFv3), Boarder Gateway Protocol versión 4 (BGP-4), Internet Protocol versión 6 (IPv6), así como los servicios WEB, FTP y SMTP con el sistema operativo Centos 6.3.

ABSTRACT

The thesis project aims to study and emulation an environment where an ISP publishes its Autonomous System which works with OSPFv3 and IPv6 over BGP-Multihoming with those services WEB, FTP and Email server.

Therefore, the work has focused on a Mulhomed solution which is focus to provide a solution when the ISP's have a disadvantage when the WAN link fail, affecting the customers deals.

Emulation seeks to clarify the theory and create a scenario that provide results like as in a real state through testing and understand the operation protocols involved. For the work development, the following steps are followed:

1. Verify the network features required to transfer the information.
2. Design the physical and logical topology.
3. IPv6 addressing scheme.
4. Configurations design according to the desired result.
5. Apply settings on the network emulation environment.

The network environment communicates through IPv6 and it has configured backup WAN links so that they work is automatically. Similarly HTTP, FTP and SMTP use the network environment through IPv6.

This project has focused on analyzing and setting an emulated environment under VMWare and GNS3 whit Open Shortest Path First version 3 (OSPFv3) , Boarder Gateway Protocol version 4 (BGP -4), Internet Protocol version 6 (IPv6) protocols and WEB , FTP and SMTP services over Centos 6.3 OS.

INTRODUCCIÓN

IPv6 se ha desarrollado durante los últimos años, el proceso ha sido impulsado principalmente por la escasez de direcciones IPv4. La crisis del espacio de direcciones IPv4 se ha visto retrasado por varios enfoques para direccionamiento IP, las más importantes son: CIDR, NAT y los espacios de direcciones privadas. Al mismo tiempo, es evidente que estas soluciones sólo posponen lo inevitable, por lo que los esfuerzos para rediseñar el protocolo IP, condujeron a IPv6.

Aunque CIDR, NAT y los espacios de direcciones privadas han tenido éxito, no resuelven el problema, sólo lo posponen. Hoy en día los Registros Regionales de Internet tienen políticas de asignación de direcciones IPv4 muy rigurosas. Los espacios de direcciones IPv4 se ha convertido en un recurso escaso y obtener un bloque de direcciones pública requiere mucho papeleo y burocracia. Se puede extender el espacio de direcciones IPv4 durante 5, 10 o 50 años, pero si el resultado es que sólo unos pocos privilegiados pueden obtener espacios de direcciones públicas no se convierte en la solución óptima.

Las especificaciones de IPv6 ahora son estables. Decenas de implementaciones se han desplegado y utilizado durante años, que ya no es necesario un software o parches especiales puesto que, la mayoría de los sistemas operativos incluyen soporte para IPv6 y algunos vendedores incluso lo activan por defecto. IPv6 ha llegado a un estado en el que casi todo el mundo puede utilizarlo. Las aplicaciones cliente-servidor, para los servidores HTTP, FTP y SMTP están incluidas en el servidor Centos para IPv6.

Con el uso de la técnica Multihoming con BGP-4, se brinda a la red redundancia y confiabilidad en el manejo de los datos. Esto significa la eliminación de todos los puntos de fallo. Con Multihoming dos o más proveedores de Internet, pueden permanecer conectados cuando se requiera y en el caso de tener problemas con una salida WAN la red no experimenta inconvenientes de comunicación.

CAPÍTULO 1
GENERALIDADES

1.1. Justificación del proyecto

El proyecto pretende satisfacer la necesidad ISP, para elevar el nivel de confiabilidad y respuesta a eventos que ofrece en sus productos de Internet y datos. Para esto, se requiere una convergencia automática a través de Multihoming de los enlaces WAN, con el fin de garantizar que los usuarios no pierdan conectividad aun cuando se presente la caída en uno de los enlaces WAN, convergiendo de una manera rápida y transparente para el usuario.

En la actualidad muchos ISP manejan un esquema manual, por medio de listas de acceso creadas en el router de core, se decide el camino por el que viajará la información al mundo, esto supone que un operador de red deberá estar presente cuando ocurra un evento sin importar la fecha y hora en la que se genere lo que demanda el uso de recursos humanos en tiempo y disponibilidad de 24 horas al día por 7 días a la semana. Además, afecta a los Acuerdos de Nivel de Servicio (SLA) que se mantienen anexados al contrato, todo esto se traduce en pérdidas para el ISP, por los descuentos que de esto se genera y pérdidas para los clientes por los negocios y transacciones que no se pueden procesar acorde al modelo de negocios que estas manejen.

Para resolver este inconveniente, la técnica de Multihoming ofrece una conmutación que se realiza de forma automática y transparente para el usuario final; a través de métricas se toma decisiones dependiendo del tipo de enlace de respaldo, capacidad y latencia al mundo.

Por otra parte, el agotamiento de direcciones IPv4 ha llevado a la implementación de técnicas como NAT (Network Address Translation), DNAT (Destination Network Address Translation), entre otras, que están en un punto de desborde en usuarios como ISP'S. Por tal razón se utilizará prefijos IPv6 que al momento no se encuentra en uso.

Se requiere lanzar un plan piloto con la publicación de un prefijo IPv6 y emular bajo el sistema operativo Centos los servicios: HTTP, SMTP, FTP. Para que en un futuro se pueda ofrecer este tipo de productos a empresas y usuarios finales. Con todo lo detallado se ayudará a tener una red más robusta e inteligente capaz de sobreponerse a fallos siendo un valor agregado al producto final que la empresa ofrece.

1.2. Objetivo General

Analizar y emular una red Multihoming a través de BGP y emular la publicación al Internet de servicios Web, transferencia de archivos y correo a través de una red IPv6, para un Proveedor de Servicios de Internet (ISP).

1.3. Objetivos Específicos:

- Investigar cómo funcionan las diferentes métricas, políticas de configuración de BGP y Multihoming para lograr un óptimo uso de recursos y manejo de datos hacia el Internet.
- Identificar las métricas que determinaran la elección del mejor camino, para la publicación de los prefijos IPv6 y su manipulación.
- Diseñar la topología de red basándose en la Ingeniería de Tráfico para dar un óptimo uso a los recursos de la misma.
- Emular Multihoming a través de GNS3, para proveer un esquema de red redundante, automático a través de 3 salidas internacionales y la publicación de la red IPv6 con servicios (Web, Transferencia de archivos y correo) a través del protocolo BGP, para probar el correcto funcionamiento del diseño.

1.4. Alcance del proyecto

El plan a desarrollarse, va a partir desde un estudio conceptual de IPv6, Multihoming, BGP y servicios: WEB, Correo Electrónico y Transferencia de Archivos, para comprender y analizar su funcionamiento.

Una vez estudiados los conceptos, se procederá con el análisis, diseño y pruebas respectivas, para así poder cumplir con todos los requerimientos de una red que requiera convergencia automática a nivel de sus salidas internacionales, basando en

la emulación de una red que puede ayudar a todos los proveedores de servicios de Internet (ISP).

Como alcance de la topología y emulación, se va a utilizar técnica de Multihoming, con tres salidas internacionales a través del protocolo BGP, se dará salida a tres servidores (emulados): WEB, Correo Electrónico, y transferencia de Datos todo esto sobre IPv6.

Dentro de los temas y puntos que no se abarcarán en el proyecto está la implementación, así como el estudio protocolos de gateway internos (IGP). Para este proyecto son transparentes topologías aplicadas en la capa de distribución y capa de acceso, ya que se enfocará en la capa de núcleo o core.

1.5. Hipótesis

Es factible la Implementación de BGP y la técnica Multihoming, para brindar redundancia automática al AS privado y sus múltiples salidas internacionales. Sobre esta plataforma, se configurará una red IPv6 con servicios: web, transferencia de archivos y correo electrónico, emulados a través de GNS3 y VMWare.

1.6. Variables e indicadores

- Escalabilidad: en el estudio, el indicador se medirá con la capacidad de adaptarse y manejar un crecimiento continuo de usuarios, sin perder la calidad en el flujo de datos. Esto con el aval de los protocolos BGP y OSPF.
- Ancho de Banda: se utilizará para medir la cantidad de datos que se pasan en un determinado rango de tiempo, en el caso de utilizar las diferentes salidas internacionales, las capacidades de enlaces contratadas arrojará resultados variables.
- Saturación: en el estudio el indicador se utilizará para futuras evaluaciones en cuanto a la capacidad mínima requerida para trabajar de una manera normal.
- Tráfico: en el estudio, el indicador se utilizará en futuras mediciones, en la evaluación y medición del consumo del conjunto de elementos que componen la red.

- Latencia: la suma de retardos temporales producidos por la continua pérdida de conexión a un determinado enlace, lo cual en una implementación real sirve para la evaluación del enlace contratado.

1.7. Población y muestra

Población: Los Proveedores de servicios de internet ISP, ubicados en la ciudad de Quito. En el continuo avance tecnológico, la demanda al Internet ha crecido de manera exponencial por lo cual, la población de la investigación se verá orientada, a los proveedores de servicio de la ciudad de Quito. Ya que el mercado es muy competitivo por la alta demanda de un servicio para hogares y la diversidad de paquetes ofertados.

Muestra: Proveedor de servicios de Internet ISP, Punto net S.A. El ISP está dentro de los principales competidores en el mercado, tanto en enlaces para hogar como en paquetes empresariales como Pymes y Corporativos. Con el fin de poder garantizar un completo estudio y optimización de recursos se ha pensado en escoger, el proveedor de servicios Punto net S.A. como modelo a seguir en el presente estudio.

1.8. Marco metodológico

La investigación será de carácter sistemático apoyada de una investigación documental.

El método sistemático está orientado a organizar y modelar el objeto en estudio mediante el análisis de sus elementos, así como los vínculos que existen entre ellos. Estos vínculos por una parte determinan la estructura del objeto y por otra su dinámica. Es una estructura de ejecución manifestada por reglas, que ayudan a llegar a tener un entendimiento sistémico de una situación dada. Para utilizar el método sistemático se deberá tener como guía los siguientes puntos:

- Entender las características primordiales del sistema (o subsistema) bajo estudio: elementos, medio, y estructura, empleados a tal fin de comprender los conceptos y prototipos básicos otorgados por el pensamiento sistémico. En los casos en los que se necesite, se considerará la posibilidad de

profundizar el conocimiento de la estructura por métodos que aporten las disciplinas relacionadas a la Teoría General de Sistemas.

- Poder distinguir entre las propiedades del sistema, cuales son resultantes que se desea obtener. (Tamayo, 2004, pág. 175)

Investigación Documental: es fundamentada en un proceso de búsqueda, recuperación, análisis, crítica y entendimiento de datos secundarios, es decir, los conseguidos y registrados por otros investigadores en fuentes documentales como: impresas, audiovisuales o electrónicas. Como en toda investigación, la finalidad de este diseño es el aporte de nuevos conocimientos. (Hochman, 1978, pág. 13)

CAPÍTULO 2
MARCO TEÓRICO

2.1 Características y limitaciones de IPv4

2.1.1 Características de IPv4

IPv4 es el protocolo de direcciones y enrutamiento de Internet que posibilita la comunicación entre cada una de las computadoras o recursos conectados a la red. Fue desarrollado en 1975, se fundamenta en las direcciones IP usuales, están conformadas por cuatro grupos de 8 bits (32 bits). (Barrios, 2009)

IPv4 brinda dos tipos de servicio: Un servicio de datos apoyado en datagramas, es decir es un servicio no fiable, que no se orienta a conexión. La otra opción de IPv4, es TCP, que está orientado a conexión y brinda la confiabilidad en los casos que se requiere. (Barrios, 2009)

El protocolo IP determina la forma en que las redes y subredes se conectan y la forma en que trabajan los dispositivos de interconexión. IP determina la manera en la que los paquetes son enrutados entre las redes y dispositivos finales; cada estación tiene una dirección IP única. Para cumplir con su trabajo los protocolos IP se apoyan en diversos juicios como son:

- DNS (Domain Name Server)
- Enrutamiento IP/Protocolos de Enrutamiento
- Direcciones Internet (Direcciones IP)
- ICMP (Internet Control Message Protocol)
- Paquetes IP

IPv4 ofrece otras funciones como la asignación de las direcciones de todos los nodos que integran la red, e identificar a un nuevo usuario que se una a la red.

Limitaciones de IPv4

Debido a la escasez de direcciones IPv4, y los problemas que esto conlleva, se espera que coexistan IPv4 e IPv6 por unos pocos años más. Dada la rapidez con la que se ha estado agotando las direcciones IPv4, la red no podrá aguantar mucho más sin este cambio.

Se puede encontrar una serie de mecanismos que permiten la coexistencia y la migración gradual de las redes así como los equipos de los usuarios, ya que es necesario el soporte de aplicaciones para videoconferencia y multimedia en tiempo real. El inconveniente que se presenta en la actualidad, es la limitación por el crecimiento exponencial de los nuevos dispositivos presentes en el mercado como por ejemplo Laptops, Tablets, Smartphones etc.

Controlar la seguridad, es un punto clave que se debe mejorar puesto que en el protocolo IPv4 es opcional. Esto debido al tipo de aplicación que se esté usando y los datos que se maneje, siempre va a ser óptima la utilización de un nivel de seguridad para la tranquilidad del usuario y el correcto manejo de la información. (Millan, 2006)

En la parte móvil resulta difícil la administración. El crecimiento de dispositivos que utilizan redes móviles obliga ampliar el rango de direcciones IPv4, el inconveniente es que a nivel mundial las direcciones IPv4 públicas se han agotado y las soluciones como NAT ya están alcanzando su límite en muchos casos.

2.2 Introducción a IPv6

Es un protocolo, que haciendo referencia al modelo OSI, se encuentra ubicado en la capa de red, al igual que IPv4 no está orientado a conexión, es decir el protocolo no tiene garantía de retransmisiones por sí mismo.

Dentro de las principales ventajas que brinda IPv6, se encuentra el amplio espectro de direcciones que admite, cerca de $6.67x10^{27}$. Si se utiliza una comparativa, 340 sextillones de direcciones por cada milímetro cuadrado de la superficie de La Tierra, versus el total de direcciones que admite IPv4 2^{23}

= 4.294.967.296 direcciones de host diferentes. (Cicileo, y otros, 2009, pág. 13)

Notación en el direccionamiento IPv6

El tamaño de las direcciones, es de 128 bits, se representan como ocho grupos de cuatro dígitos hexadecimales. Por ejemplo:

2001:0c08:85a3:07d3:1319:8a2e:0370:7224

Por otra parte, se puede comprimir un grupo de cuatro dígitos con valor 0, como se muestra en el siguiente ejemplo:

2001:0c08:85a3:0000:1319:7a2e:0370:7344
2001: 0c08:85a3::1319:7a2e:0370:7344 (Murphy & Malone, 2005, pág. 21)

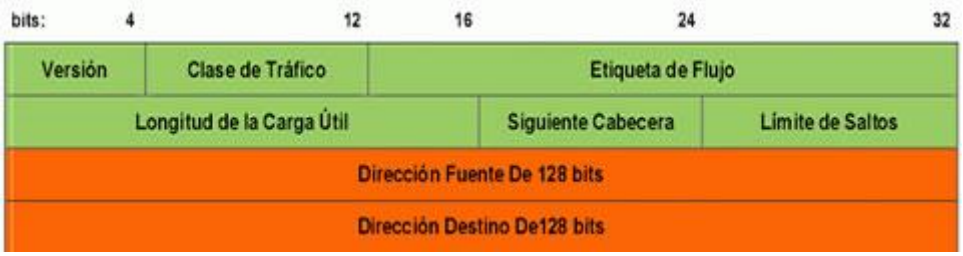
2.2.1 Paquete y Estructura de IPv6

"El paquete IPv6, está compuesto esencialmente de dos partes: la cabecera (que tiene una parte fija y otra con las opciones) y la carga útil que son los datos." (Murphy & Malone, 2005, pág. 22)

Cabecera Fija

"Los primeros 40 bytes (320 bits), pertenecen a la cabecera del paquete y contiene los siguientes campos, en la figura 1 se detalla el paquete IPv6:" (Murphy & Malone, 2005, pág. 22)

Figura 1 Paquete IPv6



Fuente: Murphy & Malone, 2005, pág. 22

Dirección de origen (128 bits): Hace referencia a la dirección IPv6 del host que originó el paquete.

Dirección de destino (128 bits): Hace referencia a la dirección de destino final del paquete.
Versión del protocolo IP (4 bits): Hace referencia a la versión del protocolo IP, en este caso su valor es igual a 6.

Clase de tráfico (8 bits): Contiene información que ayuda a los routers, a separar el tipo de tráfico al que el paquete pertenece, aplicando diferentes políticas de enrutamiento.

Etiqueta de flujo (20 bits): Maneja la Calidad de Servicio.

Longitud del campo de datos (16 bits): hace referencia al tamaño de la carga útil del paquete.

Cabecera siguiente (8 bits): Señala cual es la siguiente cabecera adicional presente en el paquete. Si no se usa, se orienta hacia la cabecera del protocolo de capa 4 utilizado.

Límite de saltos (8 bits): Hace referencia al número máximo de saltos. Este valor, es reducido en uno por cada "router" que reenvía el paquete. Si el valor se convierte en cero, entonces el paquete es descartado.

En IPv6 el fraccionamiento se hace sólo en el nodo en el que se originó el paquete, funciona a lo opuesto que en IPv4 en donde en cualquier salto, los routers pueden fraccionar un paquete. (Murphy & Malone, 2005, pág. 23)

2.2.2 Arquitectura del direccionamiento IPv6

"IPv6 tiene un espacio de direcciones, usualmente expresadas en prefijos con Classless Inter-Domain Routing CIDR para expresar la longitud de red. En la tabla 1 se realiza una descripción de los tipos de prefijos utilizados en IPv6:" (Murphy & Malone, 2005, pág. 28)

Tabla 1 Descripción general de tipos de direcciones IPv6

Prefijo	Uso Previsto
::0/96	No especificada/Loopback/compatible con loopback IPv4
::ffff:0:0:0:0:0/96	Mapeado de direcciones IPv4
200::/7	reservado para la asignación NSAP (OSI mapped prefix)
2000::/3	Global Unicast (RFC 3587)
fe80::/10	Link Local Unicast
f3c0::/10	Site-Local Unicast (Desaprobado en RFC 3879)
fc00::/7	Dirección IPv6 Local Unicast (Propuesto)
ff00::/8	Multicast

Fuente: Murphy & Malone, 2005

A continuación se explica a detalle, los tipos de direcciones IPv6:

Direccionamiento Global Unicast

"Estas direcciones son análogas a las direcciones Ipv4 públicas, la mayoría de estas direcciones se encuentran todavía reservadas, pero la asignación ya ha empezado." (Murphy & Malone, 2005, pág. 29)

En la tabla 2 se detalla los tipos de direcciones Global Unicast

Tabla 2 Direccionamiento Global Unicast

Prefijo	Uso Previsto	RFC
2001::/16	Producción a través de los Registros Regionales de Internet	RFC 2450
2002::/16	mecanismo de transición 6a4	RFC 3056
3FFE::/16	Red 6bonest	Rfc 2471,RFC 3701

Fuente: Murphy & Malone, 2005

Algunos de los espacios de direcciones están asignados para los registros regionales de Internet en grandes bloques. Los Registros Regionales de Internet RIR's son a su vez los responsables de la asignación de bloques más pequeños para los registros locales de Internet, los cuales están usualmente en

los ISP. Finalmente los ISP asignan directamente las direcciones a sus clientes.

Se espera que este esquema de asignación de direcciones jerárquica, sea la vía normal que los usuarios finales utilicen para obtener las direcciones IPv6. (Murphy & Malone, 2005, pág. 29)

Direccionamiento Link-local

El prefijo link-local contiene direcciones que representan un solo enlace. De hecho, este prefijo es usado por casi cada enlace en el que IPv6 está configurado. Esto significa que la dirección link-local fe80:: hace referencia a un equipo diferente en función de la red que esté utilizando. Al igual que 127.0.0.1 hace referencia a diferentes computadores, dependiendo cual se esté usando.

En este contexto, un enlace es un grupo de máquinas que pueden comunicarse directamente sin requerir un router IPv6. Esta conexión puede ser un punto a punto, o un enlace de broadcast pero las máquinas que usan este direccionamiento nunca pasarán a través de un router. Las direcciones link-local pueden no parecer útiles, pero estas forman parte de la autoconfiguración de IPv6.

Los hosts generan direcciones link-local en virtud de estar concatenados a un enlace, por lo que en una oficina pequeña con un switch y pocas computadoras conectadas, pueden usar el direccionamiento link-local para una red simple. Esto es una de las mayores contribuciones de IPv6 para un fácil manejo, especialmente para organizaciones pequeñas.

También es posible el uso del direccionamiento link-local cuando una dirección “real” no está estrictamente requerida. Por ejemplo, un enlace punto a punto entre dos routers podría operar solo con la dirección link-local, sin la necesidad de configurar ninguna dirección de unicast global. Sin embargo, IPv6 ha sido diseñado de manera que no debería haber escasez de direcciones y que la conservación de direcciones fuese innecesaria. También, los router

podrían requerir direcciones reales para enviar el mensaje de error ICMP o para un manejo remoto.

Configurada automáticamente la dirección link-local es en muchos aspectos, similar a la dirección IPv4 169.254.0.0/16, que es a veces empleada si el servidor DHCP no está disponible. (Murphy & Malone, 2005, págs. 29-30)

Direcciones site-local

El direccionamiento site-local, es el equivalente al direccionamiento IPv4 privado. Estas direcciones están destinadas a ser utilizados dentro de un sitio, pero no necesariamente ruteables o validas fuera de una organización a la que un espacio de dirección ha sido asignado.

A diferencia de las direcciones link-local, que sólo tienen la obligación de ser únicas en un enlace, las direcciones site-local requieren la configuración de un router que prevenga la duplicación de estas direcciones entre sitios.

Dada la clara necesidad de una dirección in-site estable, un considerable esfuerzo se invierte en conseguir la sustitución de las direcciones site-local de una manera correcta.

Un espacio suficiente de direcciones, se ha dedicado al direccionamiento site-local y unique local para asignar direcciones únicas a la mayoría de las organizaciones en el mundo. Por lo tanto, es posible que estas direcciones en realidad podrían terminar siendo válidas globalmente y enrutables. El principal problema con esto es que no está claro, cómo resolver los problemas técnicos relacionados con el enrutamiento de un espacio de direcciones no estructuradas tan grande. (Murphy & Malone, 2005, pág. 30)

Multicast

Multicast también existe en el mundo IPv4. Internet Control Message Protocol ICMP se encuentra definido en el RFC 3376 y se utiliza para gestionar grupos Multicast IPv4. Sin embargo, aunque útil, nunca ha tenido un amplio despliegue. Por el contrario, en IPv6, la multidifusión es

obligatoria, ya que es central para la operación del IPv6; ICMP se ha fusionado en ICMPv6 (RFC 2710) y es utilizada para implementar el equivalente de Address Resolution Protocol ARP de IPv6.

Multicast no requiere ninguna configuración si se limita a una única red (es decir, un solo enlace). Sin embargo, para el tráfico Multicast que se va a cruzar entre routers se debe configurar el demonio de enrutamiento de Multicast. (Murphy & Malone, 2005, pág. 31)

En la tabla 3 se detalla las direcciones utilizadas en Multicast.

Tabla 3 Direccionamiento Multicast IPv6

Alcance	Valor	Desde	Hasta
Reservado	0	ff00::/16	ff10::/16
nodo-local	1	ff01::/16	ff11::/16
link-local	2	ff02::/16	ff12::/16
site-local	5	ff05::/16	ffl15::/16
organization-local	8	ff08::/16	ffl18::/16
Global	e	ff0e::/16	ffl1e::/16
Reservado	f	ff0f::/16	ffl1f::/16

Fuente: Murphy & Malone, 2005

La lista de direcciones Multicast asignadas está disponible en el sitio web de Internet Assigned Numbers Authority IANA http:// www.iana.org/, y es relativamente largo. Sin embargo, hay dos direcciones Multicast que destacan ff02::l y ff02::2. La primera es la dirección local de vínculo para todos los nodos, y es el equivalente aproximado de la dirección de Broadcast sin enrutamiento 255.255.255.255 en IPv4. La segunda es la dirección para todos los enrutadores de enlace local, lo cual es importante en el IPv6. El proceso de configuración es automático.

Anycast

Una dirección anycast, es aquella que se encuentra entre mitad de una dirección Unicast y Multicast. Las direcciones Unicast se asignan a una máquina y cada paquete se entrega a esa máquina. Las direcciones de Multicast, son asignadas a muchas máquinas y cada paquete es entregado a

todas esas máquinas. Las direcciones anycast se asignan a muchas máquinas, pero cada paquete se entrega a una sola de estas máquinas. (Murphy & Malone, 2005, pág. 34)

2.2.3 Servicios: Web, FTP, SMTP en IPv6

2.2.3.1 HTTP en IPv6

La representación textual definida para las direcciones IPv6, no es directamente compatible con Uniform Resource Locator URL ya que usa ":" y "." como caracteres delimitadores. El RFC 2396 propone que para utilizar una dirección IPv6 en una URL, la dirección literal, debe ser encerrada entre corchete (Murphy & Malone, 2005, pág. 199).

Por ejemplo las direcciones IPv6:

FEDC: BA98: 7654:3210: FEDC: BA98: 7654:3210
1080:0:0:0:8:800:200C: 4171
3FFE: 2A00: 100:7031 :: 1

Se representaría como en el siguiente ejemplo:

http:// [FEDC: BA98: 7654:3210:FEDC:BA98:7654:3210]:80/index.html
http:// [1080:0:0:0:8:800:200C:417A] / index.html
http:// [3FFE: 2A00: 100:7031 :: 1]

Servidor Apache (HTTP) en IPv6

Apache, es un servidor web Hypertext Transfer Protocol HTTP de código abierto, es compatible con plataformas Unix (Berkeley Software Distribution BSD, GNU/Linux, etc.), Macintosh, Microsoft Windows entre otras. Usado esencialmente para enviar páginas web estáticas y dinámicas. Dentro de sus características importantes, el soporte para IPv6 en sus configuraciones, lo cual permite la adaptabilidad a nuevas funciones y características. Trabaja sobre el puerto 80 en Transmission Control Protocol TCP.

Los cambios necesarios cuando se utiliza Apache solo con IPv6 o para IPv4/IPv6 son de acuerdo a la necesidad del tipo de servidor a implementarse. Si, en la configuración se especifica que el servidor debe funcionar con una dirección IPv4 en particular, se necesita actualizar la configuración para incluir una dirección IPv6. Dentro del archivo /etc/httpd/conf/httpd.conf, la directiva Listen 80, al momento de activar IPv6 requiere el valor de [::]:80, tener en cuenta que la dirección IPv6 está encerrado entre corchetes. Con esto el servidor escucha todas las direcciones IPv4 e IPv6, a menos que IPv4 este desactivada, se escuchará sólo direcciones IPv6. Si se desea activar IPv4, se debe agregar la directiva Listen 0.0.0.0:80, la línea habilita escuchar todo el pool de direcciones IPv4. (ApacheOrg, 2013)

2.2.3.2 FTP en IPv6

El Protocolo de transferencia de archivos FTP en sus inicios, proporcionaba la capacidad de transferir información sobre conexiones IPv4. Sin embargo, con el despliegue de la versión 6 se ha realizado la adaptación para el soporte. La RFC 1639 especifica las ampliaciones de FTP, para que pueda ser utilizado en varios protocolos de red incluido IPv6. (Murphy & Malone, 2005, pág. 217)

Servidor Very Secure FTP en IPv6

Basado en UNIX, VSFTPD (Very Secure FTP Daemon) es usado para implementar servidores de archivos a través del protocolo FTP. Se diferencia porque su configuración por defecto es muy segura. En la actualidad, VSFTPD es considerado uno de los servidores FTP más seguros del mundo. Trabaja sobre TCP/IP e incluye soporte para IPv6. Utiliza los puertos 20 y 21 en TCP. (Hat, 2005)

Servicios de administración remota para FTP en IPv6

"Los servicios de administración remota son importantes, sobre todo para la configuración remota de routers y otros dispositivos. Los servicios SSH y telnet, son compatibles con Windows, IOS, Linux y la mayoría de los sistemas Unix." (BSD, 2013)

Servicios de gestión remota compatibles con FTP para IPv6

Telnetd

Como FTP, la mayoría de los vendedores y fabricantes realmente apoyan telnet a través de IPv6, la excepción principal radica en algunas versiones de Linux, que soportan solo IPv4, si bien en general se apoya a IPv6. La queja principal con telnet es que no puede encriptar las contraseñas enviadas en el inicio de la sesión, o incluso los datos que se transfiere posteriormente. Esto podría ser rectificado con IPsec, pero en general ssh es el preferido. (Murphy & Malone, 2005, pág. 35)

SSH

OpenSSH ha sido desarrollado con soporte para IPv6 desde hace mucho tiempo, por lo que Linux, BSD, y otros fabricantes que usan OpenSSH tienen un soporte maduro para IPv6. OpenSSH está disponible en http://www.openssh.com/. Si se utiliza la directiva ListenAddress, entonces es posible que se desee especificar también una dirección IPv6 con el fin de brindar una mayor seguridad al servidor, solo aceptando direcciones conocidas y confiables con las que se desee compartir la información. (BSD, 2013)

2.2.3.3 SMTP en IPv6

La adaptación de SMTP al protocolo IPv6, se basa en la traducción de DNS, los mensajes de correo de Internet se entregan generalmente, con base al sistema de nombres de dominio. El registro MX, busca conocer los hosts de destino asociados con el dominio. Se utiliza en IPv4 e IPv6, los registros IN MX en el enrutamiento de mensajes de correo. (Murphy & Malone, 2005, pág. 211)

Sendmail (SMTP) en IPv6

Sendmail comenzó a apoyar a IPv6 en la versión 8.10 y ahora se construye con soporte IPv6 en muchos sistemas compatibles de forma automática. Para habilitar el soporte en un sistema en el que IPv6 no se hayan detectado automáticamente, se puede activar la opción INET6 en sendmail.

Aparte de la construcción de sendmail con soporte IPv6, es posible que también se tenga que configurar sendmail para que escuche tanto en IPv4 e IPv6. Esto se suele hacer de forma automática si la opción NETINET6 se ha utilizado, pero se puede activar de forma explícita si es necesario mediante la adición:

DAEM0N_0PTI0NS ('Name = MTA-v4> Familia = Inet1')
DAEM0N_0PTI0NS ('Name = MTA-v6, Familia = inet6')

En el archivo sendmail.mc las direcciones IPv4 e IPv6 explícitas también pueden ser especificadas con la dirección = al campo de directivas. Por ejemplo:

DAEM0N_0PTI0NS ('Name = IPv6, Familia = inet6, address = 2001: DB8: DC: FF:: 1')

Sendmail aceptará las peticiones para escuchar las conexiones provenientes de 2001:
DB8: DC: FF:: 1. (Murphy & Malone, 2005, pág. 212)

2.3 Protocolos de enrutamiento

Los protocolos de enrutamiento brindan diferentes herramientas para proyectar y mantener las tablas de encaminamiento en los distintos routers de una red, así también define el mejor camino para llegar a un equipo remoto. Dentro de un router pueden coexistir protocolos de encaminamiento autónomos, levantando y actualizando rutas en las tablas de encaminamiento para distintos protocolos configurados.

2.3.1 Enrutamiento Estático

Se conoce como enrutamiento estático al ingreso manual de rutas en un equipo; el ruteo en el equipo no varía a menos que se ejecute el comando de configuración con diferentes parámetros. Uno de los principales inconvenientes que las tablas de enrutamiento estáticas plantean es el mantenerlas, el router no puede acoplarse por sí mismo a cambios que puedan

darse en la red. Aunque, este modo de enrutamiento resulta provechoso cuando las tablas no son muy amplias. (CISCO, 2012)

Enrutamiento Predeterminado

Pertenece al grupo del enrutamiento estático, se refiere a una conexión de salida o Gateway de "último recurso" en el caso de no tener una ruta aprendida o pre-establecida. La información enviada hacia destinos que no se encuentran en la tabla de enrutamiento se envía a dicha conexión. Es la manera más sencilla de encaminamiento para una red conectada a un único punto de salida. Para IPv4 Esta ruta se indica como la red de destino 0.0.0.0/0.0.0.0. Para IPv6 la puerta de enlace predeterminada se denota como :: /0. (CISCO, 2012)

2.3.2 Enrutamiento Dinámico

Los protocolos de enrutamiento dinámicos mantienen rutas dinámicas a través de mensajes de actualización, engloban información sobre los cambios registrados en la red y se indica al router la actualización que se debe procesar en la tabla de enrutamiento como consecuencia. El uso del enrutamiento dinámico sobre escenarios en los que no amerita, es una pérdida de canal, tiempo y dinero.

Los protocolos de enrutamiento pueden ser de dos tipos IGP y EGP.

- Protocolo de pasarela interno (IGP): se relaciona con los protocolos que se usan dentro de un sistema autónomo AS.

- Protocolo de pasarela externo (EGP): En el caso de requerir una comunicación fuera del sistema autónomo EGP, es un protocolo estándar que se utiliza para el intercambio de información de enrutamiento por medio de AS's. Los gateways en EGP sólo pueden enviar información para el acceso a redes de su Sistema Autónomo. El Gateway compila toda esta información, por medio de un protocolo IGP. (CISCO, 2011)

2.3.2.1 Protocolos de Enrutamiento Interno (IGP): RIPng, OSPFv3, EIGRP for IPv6, IS-IS

a) Routing Information Protocol new generation (RIPng)

Introducción a RIP

RIPv2 es un protocolo de enrutamiento vector distancia sin clase definido en el RFC 1721. La adición más importante a RIPv2 es la inclusión de la máscara en el paquete de actualización de enrutamiento, permitiendo al protocolo apoyarse con Variable Length Subnet Mask (VLSM) y subredes no contiguas. El protocolo resume automáticamente las rutas en los routers de frontera, aunque esta característica puede ser desactivada.

Además, RIPv2 utiliza direcciones Multicast para conseguir una mayor eficiencia en las actualizaciones periódicas en cada interfaz. Utiliza la dirección Multicast 224.0.0.9 para anunciar a otros routers RIPv2. Este enfoque es más eficiente que el enfoque de RIPv1. RIPv1 utiliza una dirección de broadcast 255.255.255.255, por lo que todos los dispositivos, incluyendo PCs y servidores, deben procesar el paquete de actualización.
La suma de comprobación del paquete en Capa 2 se lleva a cabo y luego pasa a la capa IP. IP envía el paquete User Datagram Protocol (UDP) para el proceso y UDP controla si el puerto 520 (RIP) está disponible. La mayoría de los PCs y servidores no tienen ningún proceso en ejecución en este puerto por lo cual, se descarta el paquete. El máximo número de saltos en RIP es 15, con 16 saltos la ruta es inalcanzable o no deseable.

RIP puede enviar hasta 25 redes y subredes en cada actualización y las actualizaciones se envían cada 30 segundos. Por ejemplo, si la tabla de enrutamiento tiene 1.000 subredes, 40 paquetes se envían cada 30 segundos (80 paquetes por minuto). Con cada paquete es una emisión de RIPv1, todos los dispositivos en la red reciben el paquete pero la mayoría de equipos descartan el paquete. (CISCO, 2011)

RIPng

“Al igual que RIP IPv4, RIPng es un protocolo de enrutamiento vector distancia con un límite en la métrica de 15 saltos, utiliza Split-horizon y poison reverse para evitar

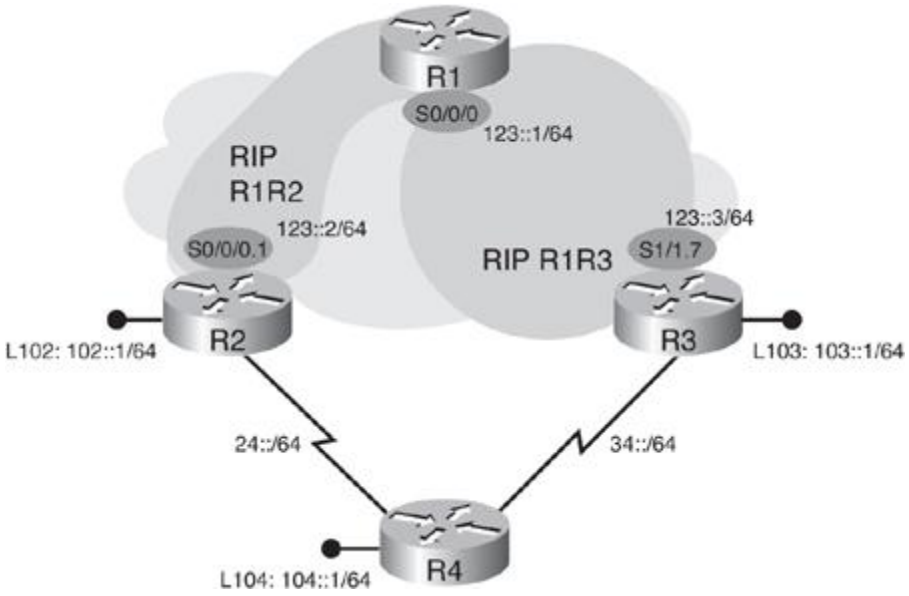
bucles de enrutamiento. Dentro de las características de IPv6 incluye:" (CISCO, 2011)

- RIPng se basa en RIP versión 2 (RIPv2) que utiliza IPv4.
- RIPng utiliza IPv6 para el transporte.
- RIPng utiliza las direcciones link-local como direcciones de origen.
- RIPng utiliza un prefijo IPv6 y una dirección de siguiente salto IPv6.
- RIPng utiliza la dirección Multicast FF02 :: 9 para todos los routers RIPng, como la dirección de destino para las actualizaciones RIPng.
- La distancia administrativa RIPng es 120.
- Las actualizaciones de RIPng se envían por el puerto 521 en UDP.

Dentro de las configuraciones de los equipos Cisco el comando *ipv6 rip* se utiliza para activar RIPng dentro de una interfaz. El parámetro *name* es el nombre del proceso de enrutamiento RIPng, que se crea automáticamente, si no existe aún, el comando *ipv6 rip* también permite, configurar el proceso de RIPng e ingresar en modo de configuración del router.

> Split-horizon es un método para evitar un bucle de enrutamiento en una red. El principio básico es simple: La información sobre el enrutamiento de un paquete en particular nunca se envía de vuelta a la dirección de la que se recibió. El comando de configuración no split-horizon router desactiva el proceso de actualizaciones de horizonte dividido en RIPng. (CISCO, 2011)
>
> El comando show ipv6 protocols, muestra los parámetros y el estado actual de los procesos de enrutamiento activos para el protocol IPv6. Adicionando la palabra clave *summary* especifica que sólo se muestren los nombres de los procesos de protocolo de enrutamiento configurados. En la figura 2 se describe un ejemplo de RIPng. (CISCO, 2011)

Figura 2 Ejemplo de una topología RIPng



Fuente: CISCO, 2011

Cada router cuenta con una dirección IPv6 configurada en la interfaz. Cabe notar que el router R1, añade los mapas a R2 y R3. En los routers R2 y R3, sólo se añade un mapa a R1.

b) Open Shortest Path First version 3 OSPFv3

Introducción a OSPF

Open-Shortest-Path-First (OSPF) es el protocolo de enrutamiento de gateway interior más usado a nivel mundial, debido a que es un protocolo de enrutamiento público (no propietario), mientras que su principal rival, EIGRP es propietario de Cisco por lo tanto otros fabricantes no lo pueden utilizar. OSPF es un protocolo de enrutamiento de estado de enlace complejo. Los protocolos de enrutamiento de estado de enlace generan actualizaciones de enrutamiento sólo cuando se produce un cambio en la topología de red. Cuando un enlace cambia de estado, el dispositivo que detecta el cambio crea un Anuncio de Estado de Enlace LSA respecto a ese enlace y envía a todos los dispositivos vecinos que utilizan una dirección Multicast especial.

Cada dispositivo de enrutamiento tiene una copia de la LSA, actualiza su Base de Datos de Estado de Enlace LSDB, y envía la LSA a todos los

dispositivos vecinos. Utiliza el puerto 89 UDP para la comunicación. (CISCO, 2011)

OSPF como el Interior Gateway Protocol lGP predilecto

La tarea de seleccionar el IGP correcto (o la combinación de IGP's) Para una red grande es difícil. Si se requiere implementar una red IP a gran escala o se tiene requerimientos inusuales, se debe analizar las variables para tomar una decisión acertada. Sin embargo, en la mayoría de pequeñas redes (hasta 99 routers) y medianas (hasta 300 routers) se toma la opción de utilizar OSPF ya que no tiene ninguna desventaja grande con los otros protocolos de enrutamiento.

Es importante tener en cuenta, el tiempo que OSPF se tarda en ejecutar el algoritmo shortest path first (SPF) y los recursos que utiliza para los cálculos de ruta, ya que delimita el número de routers y enlaces que se puede tener en una red, por que consume procesamiento y ancho de banda. Por esta razón, OSPF permite dividir su red en áreas. Cuando hay un cambio de estado de enlace, el enrutador tiene que ejecutar el algoritmo SPF sólo para el área a la que pertenece este enlace. Y es posible agregar solo la información de enrutamiento que se necesite a las tablas globales.

Existen ciertas reglas sobre la conectividad entre áreas, todas deben conectarse directamente al área 0, que es el área de red troncal, sin esta área ninguna otra sección de la red OSPF es capaz de comunicarse entre sí. Para el mecanismo de asignación de interfaces, es necesario definir rangos de direcciones IP y asignar un área. A continuación, el router reconoce la dirección IP de una interfaz y lo asigna al área asociada. Esto funciona bien si cada área tiene su propio rango de direcciones, que es un requisito previo para la agregación.

Para redes pequeñas, es mucho más fácil tener una única área y no hay restricciones en la topología, OSPF es más fácil de configurar de esta manera en cualquier red menor a 25 enrutadores; de 25 a 100 enrutadores es factible implementar en el área 0, si los routers son lo suficientemente rápidos, la red es estable, y el número de enlaces no es excesivo. Más de 100 routers en la zona 0 pueden trabajar, pero es un riesgo ya que la memoria y procesador del router pueden llegar a saturarse.

OSPFv3

OSPFv3 es una nueva implementación del protocol con soporte para IPv6. Utiliza los mismos mecanismos que OSPFv2, pero es una reescritura importante de las partes internas del protocolo.

OSPFv3 distribuye prefijos IPv6 y se ejecuta directamente a través de IPv6. Si tanto OSPFv2 y OSPFv3 se configuran en un router, se ejecutan completamente separados unos de otros y también el algoritmo shortest path first (SPF) funciona de una manera independiente. En otras palabras, los dos protocolos son como "un envío en la noche", el uno trabaja sin saber de la existencia del otro. OSPFv3 incluye las siguientes características propias de IPv6: (CISCO, 2011)

- Utiliza direcciones IPv6 de 128 bits.
- Utiliza las direcciones link-local como direcciones de origen.
- Se permite varias direcciones e instancias OSPF por interfaz.
- Soporta autenticación (mediante IPsec).
- Funciona sobre un enlace en lugar de una subred.

Se tiene que recordar que OSPF es un protocolo de enrutamiento de estado enlace.

Un enlace es una interfaz de un dispositivo de red, y un protocolo de estado de enlace toma sus decisiones de enrutamiento basado en el estado de los enlaces que conectan, los dispositivos origen y destino. El estado de un enlace es una descripción de la interfaz y su relación con sus dispositivos de red vecinos.

Para OSPFv3, la información de la interfaz incluye el prefijo IPv6 de dicha interfaz, la máscara de red, el tipo de red que está conectada, los routers conectados a la red y así sucesivamente. Esta información se propaga en diferentes tipos de anuncios de Estado de Enlace (LSA). La colección de un enrutador de datos LSA se almacena en una Base de Datos de Estado de Enlace (LSDB). El contenido de la base de datos, cuando se somete al

algoritmo de Dijkstra da como resultado la creación de la tabla de enrutamiento OSPF. (CISCO, 2011)

Similitudes entre OSPFv2 y OSPFv3

Aunque la mayoría de los algoritmos de OSPFv2 son los mismos que los de OSPFv3, algunos cambios se han hecho en OSPFv3, particularmente para manejar el aumento de tamaño de la dirección en IPv6 y el hecho que OSPFv3 se ejecuta directamente a través de IPv6. Las similitudes entre OSPFv3 y OSPFv2 incluyen las siguientes características:

Tipos de paquetes en OSPFv3

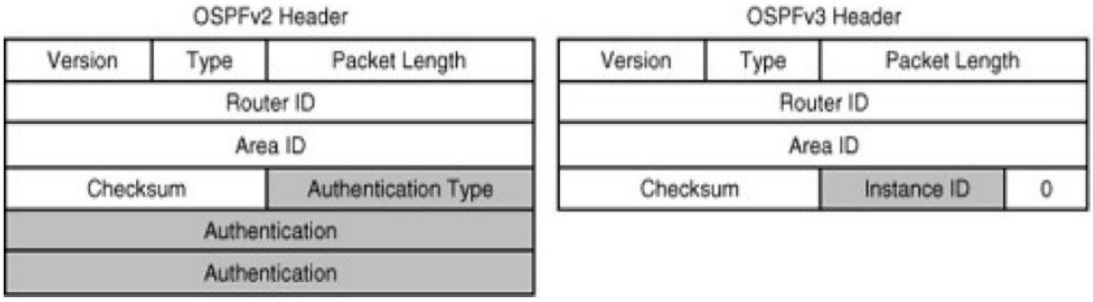
- **Hello:** los paquetes Hello en OSPF se identifican con el tipo 1. Son enviados de manera periódica en todas las interfaces, para establecer y mantener vecindades.
- **Data Base Description DBD:** los paquetes DBD se identifican con el tipo 2. Son utilizados cuando la adyacencia se está estableciendo. Contienen y describen de la base de datos de la topología.
- **Link State Request LSR:** los paquetes LSR son de tipo 3. Después de intercambiar los paquetes de DBD con un router vecino, Los LSR son intercambiados para actualizar la información de rutas.
- **Link State Update LSU:** los paquetes LSU de tipo 4. Estos paquetes aplican el envío de los LSR. Cada LSU lleva un grupo de paquetes LSU a un salto más allá de su origen. (CISCO, 2011)

Los mecanismos que se utilizan para descubrir vecinos y la formación de adyacencia son idénticos al igual que las inundaciones de LSA y tiempo agotado para las adyacencias.

Todas las capacidades opcionales de OSPFv2, áreas y las ampliaciones de Multicast para OSPF MOSPF, también se apoyan en OSPFv3. Todas las áreas deben estar conectadas al área 0, a menos que se configuren enlaces virtuales, como en OSPFv2.

OSPFv2 es muy dependiente de la dirección IPv4 para su funcionamiento, era necesario introducir cambios en el protocolo OSPFv3 para soportar IPv6, como se indica en el RFC 5340. Algunos de los cambios notables incluyen plataformas independientes de la aplicación, el procesamiento por protocolo de enlace en vez de hacerlo por nodo, soporta varias instancias por enlace y cambios en la autenticación de paquetes. Como RIPng, OSPFv3 utiliza IPv6 para el transporte y utiliza las direcciones Link-local como dirección de origen. Todos los paquetes OSPFv3 tienen una cabecera de 16 bytes, en comparación con la cabecera de 24 bytes de OSPFv2.V (CISCO, 2011)

Figura 3 Cabecera de paquetes OSPFv2 y OSPFv3



Fuente: CISCO, 2011

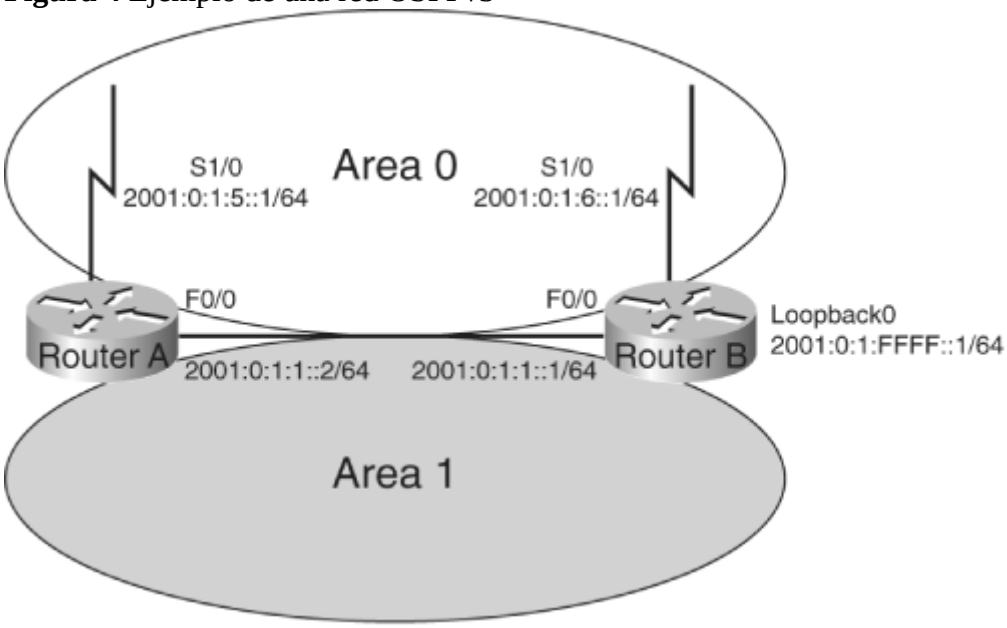
OSPFv2 no permite varias instancias por enlace, aunque una funcionalidad similar se puede obtener implementado el uso de otros mecanismos como sub-interfaces. Por el contrario, OSPFv3 tiene el apoyo explícito de varias instancias por enlace a través del campo Instance ID en la cabecera del paquete. Esta característica permite tener separados los dominios de enrutamiento, cada uno ejecutado por OSPF y utilizar un enlace común. Un solo enlace puede pertenecer a varias áreas.

La autenticación ya no es parte de OSPFv3, ahora es el trabajo de IPv6 el asegurarse que el nivel adecuado de autenticación esté en uso.

OSPFv3 usa las direcciones IPv6 Link-local, para identificar a los vecinos OSPFv3 con los que establece una adyacencia OSPFv3. OSPFv2 hace uso de la subred (o prefijo) en el que está funcionando, mientras que OSPFv3 está interesado en los enlaces a los que está conectado el router. Como se ha

comentado, IPv6 utiliza el término vínculo para indicar la facilidad de comunicación o el medio sobre el cual los nodos se pueden comunicar en la capa de enlace, las interfaces OSPF se conectan a los enlaces en lugar de subredes IP. Múltiples subredes IPv6 se pueden asignar a un solo enlace, y dos nodos pueden comunicarse directamente a través de un solo enlace, incluso si no comparten una subred IPv6 común, ya que utilizan las direcciones link-local, en lugar de las direcciones global unicast, para comunicarse. Por lo tanto, OSPFv3 corre por-enlace en lugar del comportamiento de IPv4 por-subred-IP. Y los términos *red* y *subred*, se sustituye generalmente por *enlace*. En la figura 4 se representa un enlace OSPFv3. (CISCO, 2012)

Figura 4 Ejemplo de una red OSPFv3



Fuente: CISCO, 2011

Las direcciones de multidifusión utilizadas por OSPFv3 son las siguientes:

- FF02::5 - Esta dirección representa a todos los routers OSPFv3 en el ámbito Link-local. Es equivalente a 224.0.0.5 en OSPFv2.
- FF02::6 - Esta dirección representa a todos los routers designados (DR) en el vínculo link-local. Es equivalente a 224.0.0.6 en OSPFv2.

El campo de direcciones que se encontraban en el paquete OSPFv2 se han eliminado en OSPFv3, de la siguiente manera:

- Las direcciones IPv6 no están presentes en la cabecera del paquete OSPFv3 (más bien son parte de la información correspondiente a la carga útil).
- Los routers OSPFv3 LSA y routers de red LSA no tienen direcciones IPv6.
- El router DR y el Router Designando de Respaldo (BDR) están identificados por su identificador de router, no por su dirección IP. (CISCO, 2011)

c) Enhanced Interior Gateway Routing Protocol for IPv6 (EIGRP for IPv6)

Introducción a EIGRP

Es un protocolo propietario de Cisco que trabaja en el puerto UDP 520 y combina las ventajas de los protocolos de enrutamiento por estado de enlace y vector distancia.

EIGRP tiene sus raíces como un protocolo de enrutamiento por vector distancia, es previsible en su comportamiento. Al igual que su predecesor, IGRP, EIGRP es fácil de configurar y adaptable a una amplia variedad de topologías de red. Lo que hace de EIGRP un avanzado protocolo por vector distancia y la adición de varias características de estado de enlace, como el descubrimiento de vecinos de manera dinámica. (CISCO, 2011)

EIGRP posee una rápida convergencia y la garantía de una topología libre de bucles en todo momento. Las características de este protocolo son los siguientes:

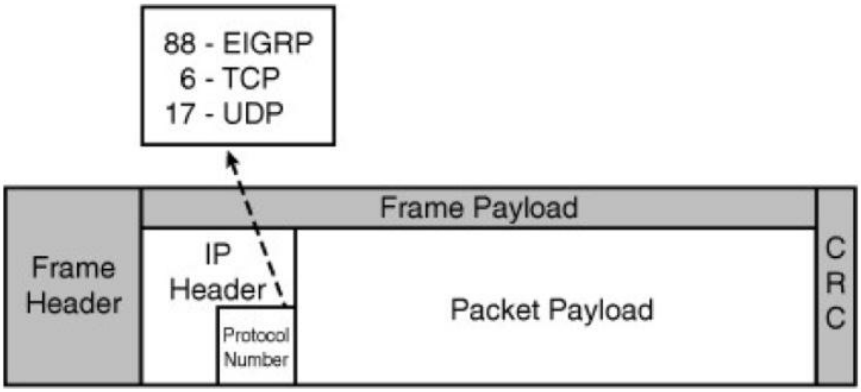
- Rápida convergencia: EIGRP utiliza Diffusing Update Algorithm (DUAL) para lograr una convergencia rápida. Un router que ejecuta EIGRP guarda en sus tablas de enrutamiento a sus vecinos para que pueda adaptarse rápidamente a los cambios en la red. Si no existe una ruta apropiada en la tabla de enrutamiento local y no existe una ruta de copia de seguridad apropiada en la tabla de topología, EIGRP pide a sus vecinos descubrir una ruta alternativa. Estas consultas se propagan hasta que una ruta alternativa se encuentra o hasta que se determina que no existe una ruta alternativa.
- Actualizaciones parciales: EIGRP envía actualizaciones parciales desencadenadas en lugar de actualizaciones periódicas. Estas

actualizaciones se envían sólo cuando la ruta o la métrica de una ruta cambia. Contienen información solo sobre el cambio del enlace en lugar de la tabla de enrutamiento. La propagación de estas actualizaciones parciales se limita automáticamente, de modo que sólo los routers que necesitan la información se actualizan. Como resultado, EIGRP consume significativamente menos ancho de banda que IGRP. Este comportamiento también es diferente del funcionamiento del protocolo de estado de enlace, que envía una actualización de cambio a todos los routers dentro de un área.

- Capa de Soporte multi red: EIGRP soporta IP versión 4 (IPv4), IP versión 6 (IPv6), AppleTalk y Novell NetWare Internetwork Packet Exchange (IPX) usando módulos de protocolo dependientes que son responsables por requerimiento específico del protocol para la capa de red. Rápida convergencia de EIGRP, sofisticada métrica de rendimiento y la estabilidad cuando se implementa en redes IP, IPv6, IPX y AppleTalk.
- Máscara de subred de longitud variable (VLSM): EIGRP es un protocolo de enrutamiento sin clase, lo que significa que anuncia la máscara de subred para cada red de destino. Esto permite a EIGRP apoyar subredes discontinuas y VLSM.
- Métrica sofisticada: EIGRP utiliza el mismo algoritmo para el cálculo de la métrica como IGRP, sino que representa valores en un formato de 32 bits, en lugar de formato de 24 bits de IGRP. Una ventaja significativa de EIGRP con respecto a otros protocolos, es su soporte para de la métrica para el equilibrio de carga desigual, que permite a los administradores una mejor distribución del flujo de tráfico en sus redes. Al igual que la mayoría de los protocolos de enrutamiento IP, EIGRP depende de los paquetes IP para entregar la información de enrutamiento.

El proceso de enrutamiento de EIGRP es una función de la capa de transporte. El paquete IP que transporta la información de EIGRP tiene el número de protocolo 88 en su cabecera IP, como se ilustra en la figura 5 (similar a la forma en que el Protocolo de Control de Transmisión (TCP), tiene como número de protocolo 6 y UDP es el número de protocolo 17). En la figura 5 se ilustra la cabecera IP correspondiente a EIGRP. (CISCO, 2011)

Figura 5 Ejemplo de la cabecera IP para EIGRP



Fuente: CISCO 2011

Eigrp en IPv6

EIGRP para IPv6 está disponible en los routers Cisco desde la versión de IOS 12.4 (6) T y posteriores. EIGRP para IPv4 y para IPv6 se configuran y gestionan por separado. Sin embargo, la configuración y el funcionamiento de EIGRP para IPv4 e IPv6 son similares.

> EIGRP para IPv6 utiliza el mismo número de protocolo (88), como lo hace EIGRP para IPv4, incluye todas las mismas características, como la información de enrutamiento de la tabla vecina de topología, y el uso de consultas si hay sucesores factibles habilitados. El ID del router es requerido para la configuración de EIGRP en IPv6. El ID del router es una dirección IPv4 32 bits. En un entorno sólo IPv6, no hay direcciones IPv4 asignadas, por lo que la ID del router se debe configurar manualmente. (CISCO, 2011)

EIGRP para IPv6 se configura en función de cada interfaz, similar a OSPFv3, el comando network para routers Cisco no se utiliza. También similar a OSPFv3, la dirección link-local se utiliza para establecer adyacencias vecinas. Por lo tanto, en EIGRP para IPv6, es posible que los routers se conviertan en vecinos, incluso si no tienen una dirección global unicast configurada.

El protocolo de enrutamiento EIGRP para IPv6, no realiza una sumarización automática como es el caso de IPv4. En equipos Cisco si se requiere realizar cualquier cambio, se debe utilizar la palabra clave IPv6 antes del comando.

d) Intermediate System-to-Intermediate System IS-IS

IS-IS es un protocolo de enrutamiento Interior Gateway Protocol (IGP) normalizado por el Internet Engineering Task Force (IETF) y de uso común en las grandes redes de proveedores de servicios. También se puede implementar en empresas que tienen redes muy grandes. IS-IS es un protocolo de enrutamiento de estado de enlace, proporciona una convergencia rápida y excelente escalabilidad. Al igual que todos los protocolos de estado de enlace, IS-IS es muy eficiente en el uso de ancho de banda de red.

Cisco es miembro activo del grupo de IS-IS en el IETF, y es responsable de muchas de las mejoras en curso en el protocolo. En los últimos años, el protocolo ha ido ganando más popularidad, con el uso generalizado entre los proveedores de servicios. Es un protocolo de estado de enlace, que permite una convergencia muy rápida con gran escalabilidad. También es un protocolo muy flexible y se ha ampliado para incorporar características de vanguardia.

IS-IS es un protocolo de estado de enlace, a diferencia de los protocolos de vector-distancia como (IGRP) y (RIP). Estado-enlace ofrece varias ventajas sobre los protocolos de vector-distancia, es más rápido en la convergencia, soporta redes mucho más grandes, y es menos susceptible a los bucles de enrutamiento. Dentro de sus características se puede mencionar: (CISCO, 2012)

- Enrutamiento jerárquico.
- Comportamiento sin clase.
- Inundación rápida de la nueva información de enrutamiento.
- Convergencia Rápida.
- Muy escalable.
- Ajuste del temporizador Flexible.
- Implementación de enrutamiento multi-área en Cisco IOS.

“(IS-IS) es una interconexión de Sistemas Abiertos Intradominio (OSI), dentro del protocolo de enrutamiento dinámico se especifica en la Organización Internacional

de Normalización (ISO) 10589. El protocolo está diseñado para funcionar en modo sin Conexión de Servicio de Red (CLNS).” (CISCO, 2012)

La función de Type Length Value (TLV)

> IS-IS, diseñado originalmente para el enrutamiento de la Interconexión de Sistemas Abiertos (OSI), utiliza parámetros TLV para transportar información de Paquetes de Estado de Enlace (LSP). Los TLV hacen IS-IS extensible. IS-IS por lo tanto pueden llevar diferente tipo de información en los LSP. IS-IS sólo admite el Protocolo de Red sin Conexión (CLNP). Sin embargo, IS-IS se prorrogó para el enrutamiento IP en el RFC 1195 con el registro de TLV 128 que contiene un conjunto de campos de 12 octetos para transportar información de IP. (CISCO, 2012)

IS-IS para IPv6

“En IPv6, IS-IS funciona de la misma manera y ofrece muchos de los beneficios que IS-IS en IPv4. Las Mejoras de IS-IS en IPv6 permiten anunciar prefijos IPv6, además de IPv4 y rutas OSI.” (CISCO, 2012)

Las Extensiones implementadas en las líneas de comando permiten la configuración de los parámetros de IPv6. IS-IS en IPv6 soporta el modo single-Topology y Multitopology, a continuación se explica su funcionamiento.

IS-IS soporte de Single-Topology para IPv6

Single-Topology soportado por IPv6, permite ser configurado en las interfaces junto con otros protocolos de red (por ejemplo IPv4). Todas las interfaces deben estar configuradas con el conjunto de familias idénticas de direcciones de red. Además, todos los routers en el área IS-IS (para el nivel 1 de enrutamiento) o el dominio (para el nivel 2 de enrutamiento) deben ser compatibles, con el conjunto de familias de dirección en la capa de red en todas las interfaces.

Cuando se utiliza el apoyo de single-topology para IPv6, se puede utilizar el antiguo o nuevo formato de TLV. Sin embargo, los TLV utilizados para anunciar la accesibilidad a los prefijos IPv6 utilizan métricas amplias. Los routers Cisco no permiten la configuración de un valor de métrica superior a 63 para la interfaz establecida, ya que por defecto está configurada para soportar la nueva versión de

TLV para IPv4. En el modo single-topology para IPv6, la métrica configurada es siempre la misma tanto para IPv4 e IPv6.

IS-IS Multitopology con soporte para IPv6

IS-IS multitopology con soporte para IPv6 permite mantener un conjunto de topologías independientes dentro de una misma área o dominio. Este modo elimina la restricción de que todas las interfaces en las que IS-IS este configurado, se debe apoyar el conjunto idéntico de familias de direcciones de red. También elimina la restricción de que todos los routers en el área de IS-IS (para el nivel 1 de enrutamiento) o de dominio (para el nivel 2 de enrutamiento) deben ser compatibles con el conjunto idéntico de familias de direcciones de la capa de red. Debido a que se realizan múltiples Shortest Path First (SPF's), uno para cada topología configurada es suficiente, ya que existe conectividad entre un subconjunto de los routers en la área o dominio de una familia de direcciones de red, para ser enrutable.

El comando isis ipv6 metric permite configurar diferentes parámetros en una interfaz de IPv6 e IPv4.

2.3.2.2 Border Gateway Protocol version 4 (BGP-4)

> BGP utiliza TCP en el puerto 179 para la comunicación con los vecinos. Esto es inusual ya que el resto de protocolos de enrutamiento corren directamente sobre IP o utilizan UDP. Esto hace que sea posible el envío de broadcast o Multicast para descubrir los routers vecinos. La funcionalidad de descubrimiento de vecindades no se requiere para BGP, sin embargo, por lo que se ejecuta a través de TCP, evita tener que incorporar una cantidad significativa de las funcionalidades del protocolo de transporte, tales como la fragmentación, la secuenciación, y la retransmisión de los datos.
>
> Las Versiones de BGP 1, 2, y 3 deben ser consideradas completamente obsoletas. Siempre que se utilice "BGP", significa BGP-4. (CISCO, 2012)

Cuando se establecen vecindades en BGP con una sesión TCP, comienza el intercambio de información BGP en forma de "mensajes". Cada mensaje comienza

con una cabecera, seguido por el contenido del mensaje, como se muestra en la tabla 4.

Tabla 4 Formato de encabezado del mensaje BGP

Marker	Length	Type	Message contents
16 bytes	2 bytes	1 byte	0 - 4077 bytes

Fuente: BGP ,2002

El campo Marker normalmente contiene solo un segundo 1 y se utiliza para comprobar si el remitente y el receptor están todavía sincronizados. Si el receptor se encuentra con un valor inesperado en el campo de marcador, algo debe haber salido mal, por lo que el receptor envía una indicación de error y cierra la conexión. El campo Length contiene la longitud del mensaje BGP, su valor mínimo es 19 bytes (sólo un encabezado con ningún mensaje) y un máximo de 4.096 bytes. Type indica el propósito del mensaje: open (1), update (2), la notificación (3) o Keep Alive (4) (tal como se define en el RFC 1771).

Open Message

Ambas partes envían un Open Message inmediatamente después de que se ha establecido la sesión TCP. El mensaje transmite información importante acerca de la configuración y las habilidades de BGP. En la siguiente tabla se muestra el formato del mensaje. En la tabla 5 se detalla el formato del paquete Open Message de BGP.

Tabla 5 Formato de Open Message de BGP

Versión	My AS	Hold time	Identifier	Par len	Optional parameters
1 byte	2 bytes	2 bytes	4 bytes	1 byte	0-255 bytes

Fuente: BGP, 2002

El primer campo indica la versión de BGP, que normalmente sería 4. El siguiente campo es el número de AS del remitente. Hold time (Tiempo de espera) es el número máximo de segundos, que la sesión puede permanecer inactiva antes de ser cerrada debido al agotamiento del tiempo. El tiempo mínimo de espera es de tres segundos, el valor cero significa que la sesión no expirará. El campo Identifier

contiene una de las direcciones IP de BGP. Un router debe utilizar el mismo identificador para todas las sesiones BGP. El campo opcional longitud de parámetro ("par len") indica la ausencia (con un valor de cero) de información en este campo. Si hay cualquier parámetro opcional, todos ellos están precedidos por un tipo de parámetro de un byte y una longitud de parámetro de un byte. Los parámetros opcionales se utilizan para poder negociar el uso de autenticación y capacidades extendidas como las extensiones de multiprotocolo y actualización de ruta.

Si el contenido de open message satisface el requerimiento del router, este envía un mensaje keepalive e inicia el envío de una copia de la tabla de enrutamiento de BGP (en la medida en que las políticas configuradas lo permiten) con mensajes de actualización. Una vez completado esto, el router envía solamente mensajes de actividad periódicos y actualizaciones incrementales si hay algún cambio en la tabla de enrutamiento.

Update Message

Update Message retira y agrega nuevas rutas. Ambas son opcionales y configurables.

Tabla 6 Formato de Update Message

UR length	Withdrawn routes	PA length	Path attributes	NLRI
2 bytes	Variable	2 bytes	Variable	Variable

Fuente: BGP, 2002

El campo longitud de las rutas no alcanzables ("UR length ") especifica la longitud del campo a ser retirado; cero significa que este campo está ausente.

El campo withdrawn-routes muestra todas las rutas que ya no son accesibles. No hay necesidad de retirar explícitamente una ruta cuando los atributos cambian.

Un mensaje de actualización con los nuevos atributos y NLRI (capa Network Layer Reachability Information) es suficiente.

Cada ruta retirada consiste en un campo de longitud, que indica la longitud del prefijo (en bits), y bytes suficientes para mantener el prefijo. Todos comienzan con un byte que contiene indicadores de atributo y un segundo byte que indica el tipo de atributo.

Notificación y mensaje Keepalive

Se genera un mensaje de notificación cuando se presenta una condición de error fatal. Después de transmitir la notificación, el router que envía cierra la conexión TCP. El mensaje consiste en un código de un byte de error, un subcódigo de error de un byte, y los datos opcionales, se envían mensajes keepalive de conexión, cuando se detecta que la conexión está inactiva, para asegurarse de que el temporizador de espera no caduque. (Van Beijnum, 2002, pág. 19)

Estados de BGP

Dentro de RFC para BGP se tiene una lista de estados específicos en que una sesión puede estar, así como un diagrama de transición de estado (la "máquina de estados finitos" de BGP). El comportamiento del router está obligado por el estado de una sesión BGP, La Management Information Base (MIB) de BGP define un mensaje de captura para SNMP, que puede ser enviado cuando una sesión pasa de un estado "alto" en un estado de "inferior". Estos estados son los siguientes: (Van Beijnum, 2002, pág. 19)

- **Idle:** el router no está tratando de establecer una sesión BGP, y si el vecino intenta crear una sesión, se rechaza la conexión TCP. La ruta espera un evento "start", por lo general el usuario habilita BGP o añade a un vecino o una interfaz.
- **Connect**: en este estado, el router espera el intento de establecer una sesión TCP para completar una conexión y escucha las sesiones TCP entrantes.
- **Active:** BGP está esperando una sesión TCP.
- **OpenSent**: open message ha sido enviado, pero aún no se ha recibido del vecino.
- **OpenConfirm:** open message ha sido recibido desde el vecino, pero aún no el mensaje keepalive que completa la fase de establecimiento de la sesión BGP.
- **Established**: el mensaje keepalive se ha recibido, y la sesión está lista para la transmisión de la actualización, keepalive y mensajes de notificación. (Van Beijnum, 2002, pág. 20)

El estado de cada vecino se muestra en el resultado del comando *show ip bgp summary* como el último elemento en la línea y la información específica del vecino.

Si el router muestra el número de prefijos recibidos, está "establecido".

Propagación de las rutas en BGP

Cuando un router recibe una nueva ruta en un mensaje de actualización de BGP, se ejecuta el siguiente procedimiento:

1) Comprueba todos los filtros entrantes definidos para la sesión BGP. Si la ruta no se permite a través de uno de los filtros, se ignora, y el procedimiento se detiene.
2) Inserta la ruta en la tabla de BGP.
3) Compara la ruta a otras rutas de la tabla de BGP con el mismo destino, prefijo Network Layer Reachability Information (NLRI), y ejecuta el algoritmo de selección de ruta para BGP. Si la nueva ruta no se considera la mejor ruta, el procedimiento se detiene.
4) Considera que la nueva mejor ruta y la incluye en la tabla de enrutamiento. Se retira la ruta vieja por la mejor ruta.
5) Propaga la nueva mejor ruta a los vecinos BGP en los sistemas autónomos externos, si los filtros configurados por el vecino lo permite.
6) Propaga la nueva mejor ruta a los vecinos BGP en el AS local, como si esa ruta no fue recibida de otro vecino BGP en el AS local. (Por lo general, no existe un filtrado entre vecinos BGP dentro de un el mismo AS.) (Van Beijnum, 2002, pág. 26)

2.4 Multihoming

“El término Multihoming se refiere a la práctica que se tiene con los proveedores de la red y los proveedores de acceso a Internet, cuando se conecta con más de un enlace.” (Van Beijnum, 2002, pág. 78)

Un Sistema Autónomo con Multihoming mantiene la conexión a Internet, cuando se tiene un fallo o pérdida en una de las conexiones y es capaz de dirigir el tráfico a

cualquier destino por medio de otra conexión, entregando un mejor servicio y previniendo la saturación en el destino.

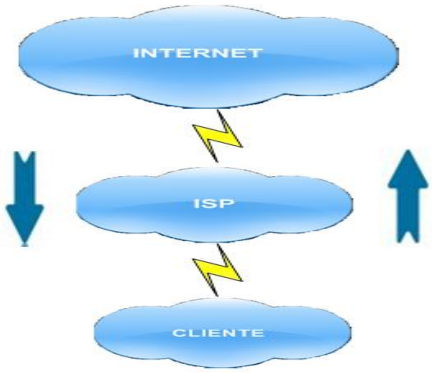
Se emplea especialmente para fines en los que se requiere la implementación de redundancia, con perspectivas de garantizar la calidad en el servicio. Las empresas necesitan cada vez más de una conectividad hacia el Internet, lo que conlleva a la necesidad de considerar adquirir un nivel de redundancia de proveedores de acceso (Multihoming), con el fin de asegurar la conectividad hacia Internet cuando se necesite.

Formas de conexión con Multihoming:

Múltiples conexiones utilizando un solo Proveedor de Servicio

Consiste en la conexión de un único router de borde de Internet hacia dos o más routers distintos de un único Proveedor de Servicio de Internet.

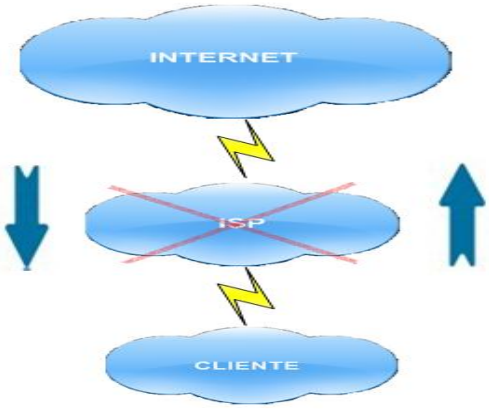
Figura 6 Multihoming



Elaborado por: Fausto Flores

En el momento en que la conexión al Proveedor de Servicio de Internet o el enlace físico se pierde y el Internet deja de funcionar, la organización queda incomunicada y sin Acceso hacia el internet, convirtiéndose en una pérdida independientemente del modelo negocio que se maneje.

Figura 7 Multihoming pérdida de enlace

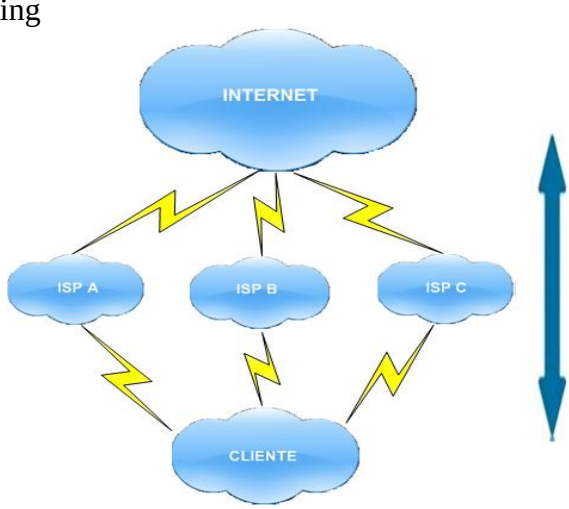


Elaborado por: Fausto Flores

Múltiples conexiones con varios Proveedores de Servicio

Con el fin de dar redundancia a la red hacia el Internet y se pueda evitar la pérdida de conexión o reducir la probabilidad de que se dé, se utiliza una conexión a varios ISP's. Lo que Garantiza subir el nivel en la disponibilidad, ya que es menos probable que dos o más servicios totalmente independientes colapsen al mismo momento.

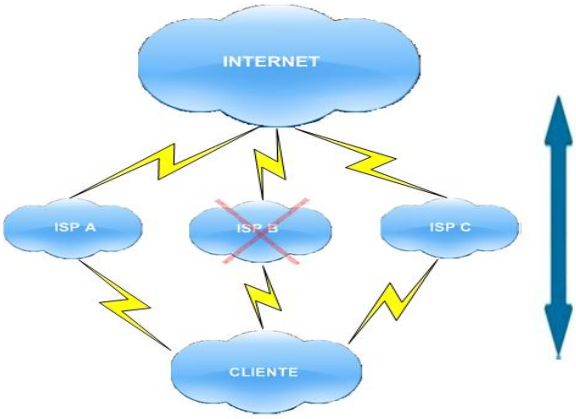
Figura 8 Multihoming



Elaborado por: Fausto Flores

Con el uso de la topología mostrada en la figura 9, si el enlace en uno de los proveedores falla, la organización continua con conexión hacia el Internet a través de los otros ISP's, ya que de manera automática el protocolo selecciona otra vía de comunicación hacia el Internet.

Figura 9 Multihoming pérdida de conexión hacia un ISP



Elaborado por: Fausto Flores

BGP y Multihoming con soporte para IPv6:

Se dice que un ISP tiene implementada una solución Multihoming, si obtiene conexión a Internet a través de dos o más Proveedores de Servicio. Esencialmente, este medio es empleado para mejorar en uno o varios aspectos la calidad de la conectividad a Internet. El más relevante es la tolerancia a fallos.

"En la actualidad, BGP está dentro de los principales protocolos empleados para lograr redundancia hacia el Internet. Multihoming ofrece redundancia y optimización de la red, ya que selecciona el mejor camino para el viaje de datos". (Van Beijnum, 2002, pág. 79)

Existe muchas razones por las que un ISP desearía estar conectado a múltiples proveedores de servicio, aunque en la práctica no todas las implementaciones brindan todas las ventajas, a continuación se detallan algunas características que ofrece la implementación de Multihoming:

- **Tolerancia a fallos:** un ISP en el que se ha implementado Multihoming, es "inmune" a la pérdida de conexión hacia el mundo. Es decir, si detecta una falla que afecta la comunicación, debería ser capaz de enviar el tráfico a través de otro proveedor que se encuentre operativo.
- **Balanceo de carga:** multihoming admite distribuir el tráfico entrante y saliente entre los distintos proveedores de servicio, a los que se está conectado. De modo que se tiende a maximizar el uso de los recursos.

- **Ingeniería de tráfico:** el ISP puede determinar, en alguna medida, el tipo y volumen de tráfico a enviar a cada Proveedor de servicio, apoyándose en aspectos tales como los acuerdos de nivel de servicio (SLA), costos de conexión o en otras políticas definidas.
- **Independencia de los Proveedores de Servicio:** por lo regular, un ISP busca no depender de los Proveedores de Servicio, para poder disfrutar de las ventajas de Multihoming. Es la razón por la que, las soluciones de Multihoming acostumbran tener en cuenta que no se requiera ningún tipo de asistencia especial por parte de los proveedores para implementarlas. Esto conlleva a que cada ISP pueda ocupar distintos Proveedores de Servicio de forma libre e implementar Multihoming por cuenta propia. (Van Beijnum, 2002, págs. 80-81)

Por último, un aspecto fundamental a considerar en la configuración de un AS multihomed es que este AS, no funcione como Sistema Autónomo (AS) de tránsito para el tráfico que proviene de Internet, de manera que toda la información que viaje por el AS sea local. Para ello, no se debe anunciar hacia el exterior ninguna ruta que no tenga origen en este AS, ya que anunciar una ruta implica aceptar todo el tráfico que tenga como destino esa ruta. Así, una tarea obligatoria en esta configuración sería filtrar las rutas recibidas por un Proveedor de Servicio para que éstas no sean anunciadas hacia otro ISP. Por lo cual, las listas de acceso, son las llamadas a realizar este trabajo. (Van Beijnum, 2002, pág. 83)

2.5 Ingeniería de tráfico en bgp -4

La ingeniería de tráfico, es la forma en que se gestiona la red, a partir de los Path Attributes (PA) con los que cuenta y la adaptación del protocolo para satisfacer las características de un escenario BGP. Para esto, se fijan características para el tráfico saliente y entrante, siendo este último un poco más difícil de controlar. De modo que este manejo se hace a partir de la elección de las rutas que cualquier router, va a anunciar en una red y de las rutas que va a elegir como preferentes y alternativas. (Van Beijnum, 2002, pág. 95)

Se tiene un conjunto de Path Attributes (PA), que aportan información, para la toma de decisiones de filtrado o selección de rutas. A continuación se describen los principales PA:

- **ORIGIN:** describe el mecanismo por el cual el prefijo IP se anunció por primera ocasión. Se especifica como: Interior Gateway Protocol (0), Exterior Gateway Protocol (1) o INCOMPLETE (2). Interior Gateway Protocol señala que el prefijo IP fue aprendió por un protocolo dentro del sistema autónomo como por ejemplo EIGRP, Exterior Gateway Protocol señala que el prefijo IP fue aprendido por un protocolo exterior como BGP. Generalmente si el ORIGIN es 2, se ha aprendido de forma estática.
- **AS-PATH:** Path Attribute (PA) reúne una serie de números de AS que identifican los caminos de ASs por los que ha atravesado el anuncio. En Cada ocasión, en la que un router de borde difunde una ruta hacia otro lado, añade su número de AS a este atributo, constituyendo así la lista de AS's. La lista no se modifica si se usa IBGP. Si se desea emplear AS-PATH como método de selección de rutas, se debería escoger la lista AS-PATH de menor tamaño.
- **NEXT-HOP:** se refiere a la dirección IP del router que hace referencia al siguiente salto, en dirección al destino. Hay que tomar en cuenta que un prefijo IP se publica hacia afuera del sistema autónomo, entonces el NEXT-HOP es el destino que se conoce y por donde se tiene que enviar el tráfico de los usuarios que desean llegar a una dirección final. La información del NEXT-HOP se procesa de acuerdo a los datos de tabla de enrutamiento IP. Ahora se tendrá una tabla IP (la que ya se tenía anteriormente) y una tabla BGP que contendrá el NEXT-HOP para alcanzar cada destino.
- **MULTI-EXIT-DISCRIMINATOR (MED):** es un indicador planeado para ser empleado cuando desde un sistema autónomo se tiene múltiples enlaces hacia otro sistema autónomo. Este atributo se puede utilizar para balanceo de carga, Esta métrica es local en medio de dos sistemas autónomos, no se propaga fuera de ese espacio.
- **LOCAL-PREF:** Path Attribute (PA) es provechoso, en un marco en el que un sistema autónomo tiene conexión con múltiples sistemas autónomos, de

modo que puede haber diversas rutas hacia un mismo destino. Este atributo dará prioridad al envío de datos por un enlace determinado, por tanto solo tendrá validez dentro del sistema autónomo, luego solo se traspasa por IBGP. Se elegirá el envío de la información por la ruta que tenga un LOCAL-PREF mayor, el LOCAL-PREF por defecto tiene un valor de 100. (Van Beijnum, 2002, pág. 108)

Selección de una ruta

El conjunto de los atributos mencionados en la Ingeniería de tráfico, pueden ser empleados simultáneamente para la selección de rutas, por otro lado se debe implantar un orden de prioridad de manera que si se existen diversas rutas que se puedan tomar como preferentes, solo se elija una. Se pasará a la siguiente lista y se suprimirá las rutas que no concuerdan con el mejor valor de cada uno de los criterios. Se debe tener en cuenta, que los criterios para escoger la decisión en el encaminamiento, que abarcan normas de desempate se sujetan a cada prefijo IP o al conjunto de prefijos IP destino. A continuación se detallan los pasos que se sigue para la elección de una ruta:

1) En el caso de que el siguiente NEXT-HOP no se encuentre disponible se descarta la ruta.
2) Se Eliminan las rutas que tienen menor LOCAL-PREF.
3) Se Eliminan las rutas que tienen AS-PATH más extenso.
4) Se Eliminan las rutas que tienen ORIGIN más alto.
5) Se Eliminan las rutas que tienen mayor MED.
6) Se Eliminan las rutas que se han aprendido por IBGP, en el caso de que existan rutas aprendidas por EBGP.
7) Se Eliminan las rutas que tienen mayor coste hacia el NEXT-HOP.
8) Se prefiere la ruta que ha sido anunciada por el router que tiene el menor identificador de BGP.
9) Se prefiere la ruta que ha sido recibida desde la interfaz con la menor dirección para el vecino. (Van Beijnum, 2002, pág. 109)

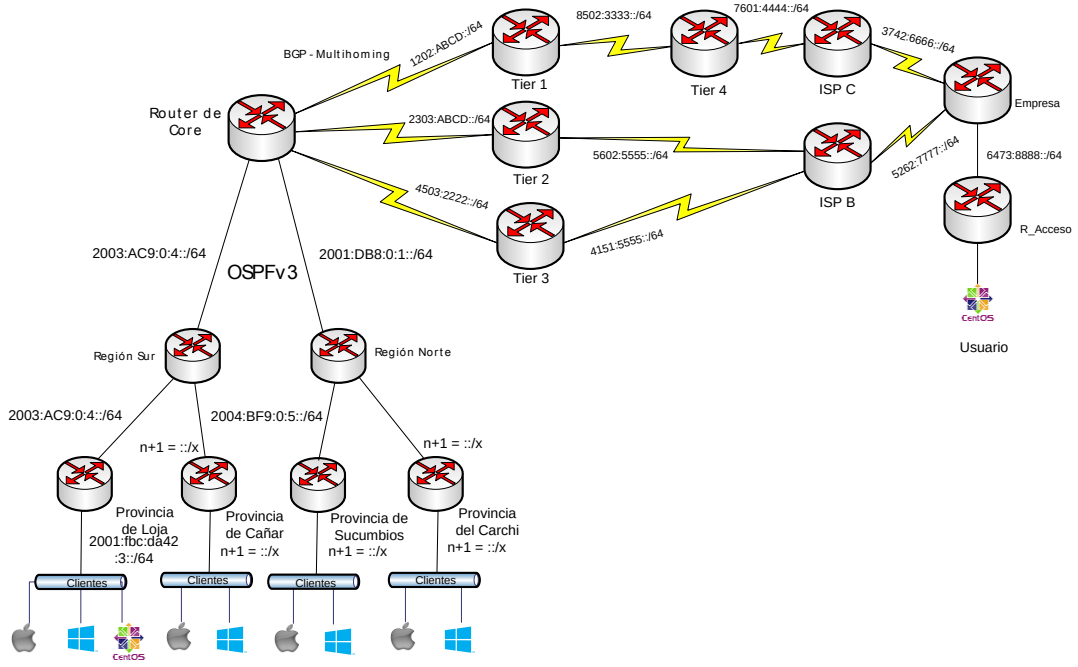
CAPÍTULO 3
DISEÑO

3.1 Topología de red y direccionamiento ipv6

El diseño de la topología, implica adaptar los equipos de la red al ambiente de trabajo, de tal manera que los recursos de la red sean aprovechados optimizando tiempo, recursos y dinero.

En este trabajo, el Proveedor de Servicios de Internet ISP, tiene cobertura a nivel nacional, el medio de transmisión con el que interconecta las ciudades es independiente en la emulación, es decir no influye en la topología lógica. Las provincias se interconectan a dos concentradores el primero ubicado en la ciudad de Quito y el segundo en la ciudad de Guayaquil, la primera ciudad controla la región norte y la segunda las provincias de la región sur. En la figura 10 se encuentra la topología del ISP incluyendo tres salidas internacionales de respaldo.

Figura 10 Topología del ISP



Elaborado por: Fausto Flores

El diseño de la topología está dividido en tres grupos de acuerdo al tipo de tecnología que se haya manejado para la implementación:

- **Acceso**: es la interconexión de los clientes con el ISP, una vez enrutada la IP asignada el cliente puede tener acceso a los diferentes servicios que se ofrece, así como al Internet.
- **Sistema autónomo AS:** en esta capa se mantiene la gestión de la comunicación, para los sitios remotos que componen al sistema autónomo.
- **Core**: es el concentrador donde converge OSPFv3 y BGP-4. En este equipo o equipos se conectan los enlaces de respaldo y principal que brinda la salida hacia el internet y se crean políticas de enrutamiento que dependen de las necesidades de la red.

Para realizar la emulación de Multihoming a través de IPv6 se debe realizar los siguientes pasos:

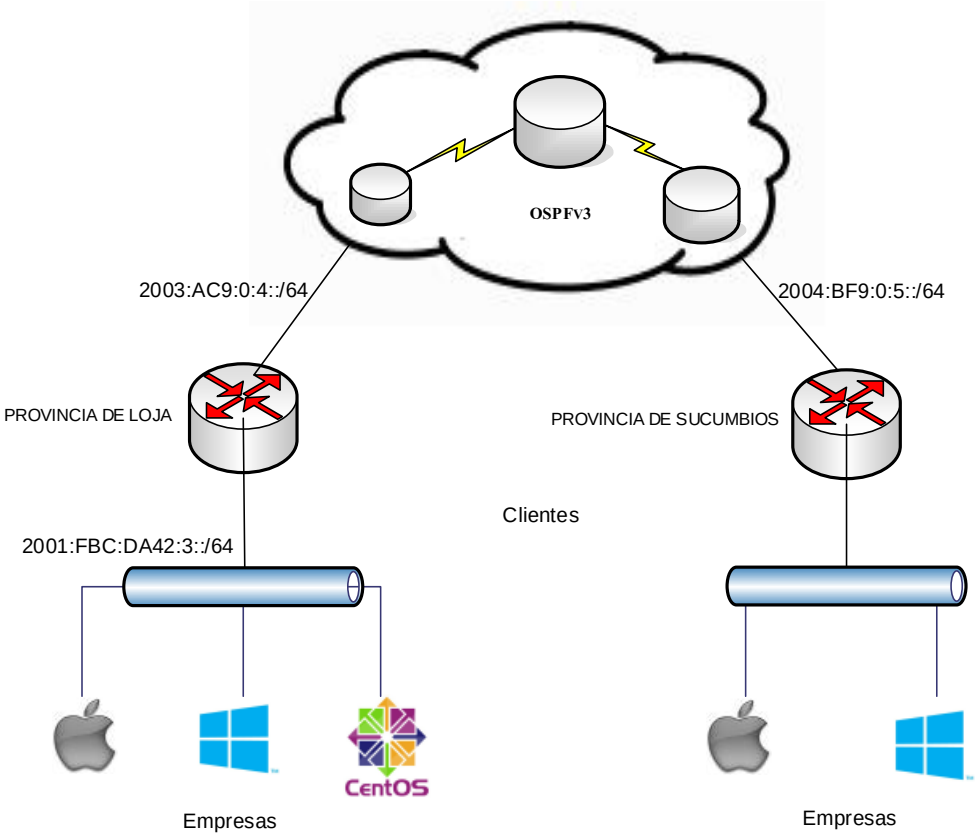
- Instalar los emuladores: GNS3 y VMWare.
- Montar las versiones de Cisco y Linux con soporte para IPv6.
- Direccionamiento IPv6
- Configuración de Servicios y Equipos.
- Aplicar políticas de enrutamiento.

3.1.1 Topología de la red de área red local LAN y Direccionamiento IPv6

La topología LAN, es el ambiente en el cual el usuario se desarrolla, por lo tanto para una empresa es imperante planificar un diseño acorde a las necesidades del modelo del negocio.

Como alcance al presente trabajo, se ha implementado un servidor Centos 6.3 y configurado los servicios: WEB, FTP y SMTP con el fin de emular solicitudes desde un cliente remoto.

Figura 11 Topología de red LAN



Elaborado por: Fausto Flores

Requisitos para la emulación de LAN de acuerdo a la topología descrita en la figura 11:

- Instalar el servidor Centos 6.3 en VMWare: La elección de este sistema operativo se debe a que dentro de sus características destaca el fácil mantenimiento y soporte a largo plazo para sus aplicaciones. En la versión DVD tiene la gran mayoría de los paquetes necesarios para la configuración de servicios. En la herramienta VMWare se ha emulado el sistema operativo Centos 6.3 con los servicios HTTP, FTP y SMTP para un cliente en la Provincia de Loja.
- Un router Cisco 7200 con soporte para IPv6 emulado sobre GNS3. GNS3 además de ser gratuito es uno de los emuladores más completos en el mercado y ofrece todas las ventajas de un equipo real.

Direccionamiento IPv6 para la red LAN:

El tipo de direccionamiento aplicado en la topología es GLOBAL-UNICAST ya que es análogo a las direcciones IPv4 públicas, lo cual implica que la dirección puede ser alcanzada desde cualquier parte del mundo. Si el cliente desea publicar servicios, no se tendrá inconvenientes al momento de hacer uso de los recursos implementados. En la tabla 7 se muestra el direccionamiento IPv6 del servidor.

En la emulación del proyecto los prefijos de subred siempre contienen 64 bits. Estos bits contienen 48 que corresponden al prefijo de sitio y además 16 bits para el ID de subred.

Tabla 7 Direccionamiento IPv6 servidor –Gateway

Router	**IP**	**Tipo de Dirección**	**INT**
Servidor	2001:FBC:DA42:3::2	GLOBAL-UNICAST	fa1/0
Gateway	2001:FBC:DA42:3::1		fa1/0
RED	**Prefijo**	**Rango**	
2001:fbc:da42:3::	/64	**Desde**	**Hasta**
	/64	2001:0fbc:da42:0003::	2001:0fbc:da42:0003:ffff:ffff:ffff:ffff

Elaborado por: Fausto Flores

3.1.2 Topología OSPFv3

En la emulación el Proveedor de servicios ISP tiene cobertura a nivel nacional, por lo cual se ha divido al país en dos zonas: Norte y Sur.

El concentrador OSPFv3 zona norte está ubicado en Quito, se compone por las provincias que se listan en la tabla 8.

Tabla 8 Provincias concentrador zona norte

Orden	Provincia
1	Pichincha
2	Sto. Dgo. Tsáchilas
3	Cotopaxi
4	Tungurahua
5	Pastaza
6	Napo
7	Orellana
8	Sucumbíos
9	Imbabura
10	Esmeraldas
11	Carchi

Elaborado por: Fausto Flores

El concentrador OSPFv3 zona sur está ubicado en Guayaquil, se compone por las provincias que se listan en la tabla 9.

Tabla 9 Provincias concentrador zona sur

Orden	Provincia
1	Manabí
2	Los Ríos
3	Guayaquil
4	Bolívar
5	Chimborazo
6	Cañar
7	Morona Santiago
8	Azuay
9	El Oro
10	Loja
11	Zamora Chinchipe
12	Santa Elena

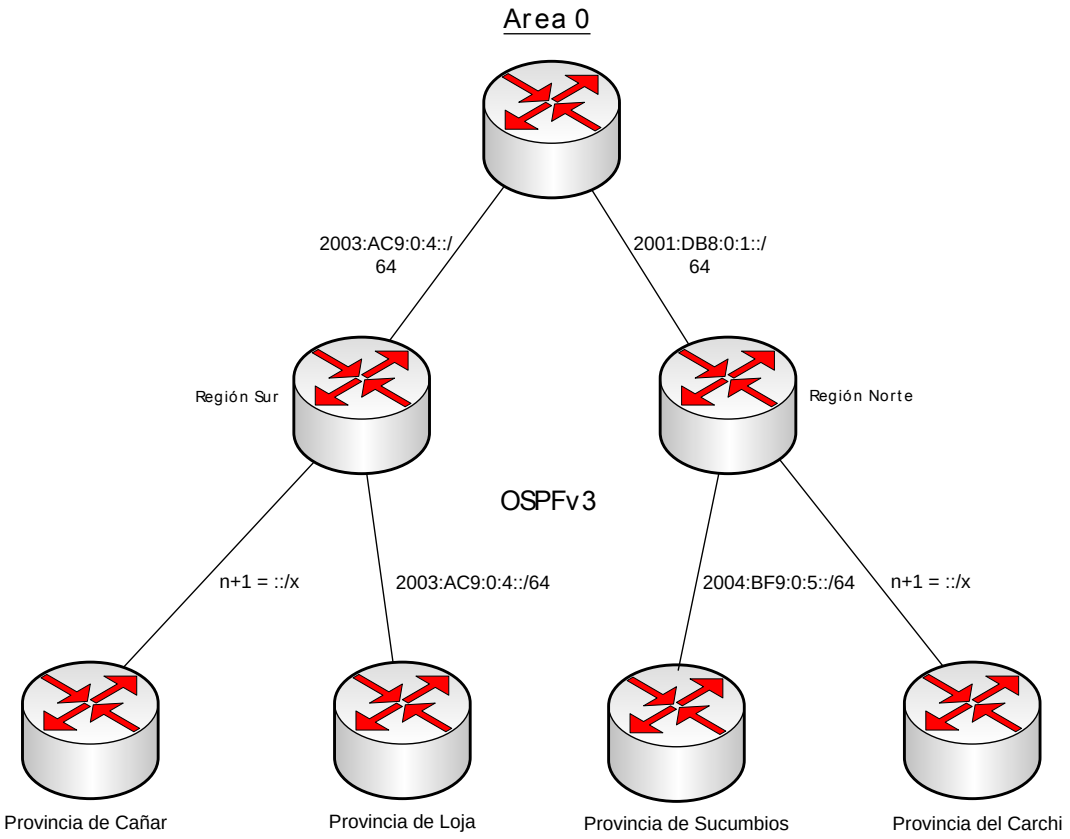
Elaborado por: Fausto Flores

Al dividir el tráfico en dos concentradores, el flujo de datos en los routers OSPFv3 ubicados en Quito y Guayaquil, se maneja de una mejor manera aportando escalabilidad y mayor tolerancia a fallos.

Sobre el área 0 de OSPFv3, se ha realizado la configuración de los equipos, ya que la cantidad de routers conectados no demandan configurar otra área. Se puede

trabajar en el área 0 con un número de dispositivos de 25 a 100 enrutadores sin tener que hacer uso de otra área.

Figura 12 Topología OSPFv3



Elaborado por: Fausto Flores

Se ha seleccionado OSPFv3 que posee las siguientes características:

- Fácil adaptabilidad a nuevos nodos (sucursales ubicadas en provincias).
- Fácil mantenimiento de la red: es un protocolo dinámico.
- Fácil mantenimiento de las tablas de rutas para todos los equipos que participan de OSPFv3.
- Rápida convergencia de datos: en el caso de que un enlace falle y se recupere, automáticamente la conexión regresa a su estado normal.
- Libre de lazos de red: el protocolo bloquea las rutas que pueden afectar el flujo de la información, generadas por una configuración errónea.
- Menor número de administradores de red: la configuración se realiza una vez en cada dispositivo, si un cambio de enrutamiento es requerido solo se difunde la ruta hacia todo el Sistema Autónomo.

La tabla 10, hace referencia al direccionamiento IPv6, correspondiente al concentrador de Quito y su conexión con el router de core:

Tabla 10 Direccionamiento IPv6 Core-MTZ_UIO Quito

Router	**IP**	**Tipo de Dirección**	**INT**
Core	2001:DB8:0:1::1	GLOBAL-UNICAST	Fa 1/0
MTZ_UIO	2001:DB8:0:1::2		
RED	**Prefijo**	**Rango**	
2001:db8:0:1::	/64	**Desde**	**Hasta**
		2001:0db8:0000:0001::	2001:0db8:0000:0001:ffff:ffff:ffff:ffff

Elaborado por: Fausto Flores

La tabla 11, hace referencia al direccionamiento IPv6, correspondiente al concentrador de Quito y su conexión con la provincia de Sucumbíos:

Tabla 11 Direccionamiento IPv6 MTZ_UIO-Sucumbíos

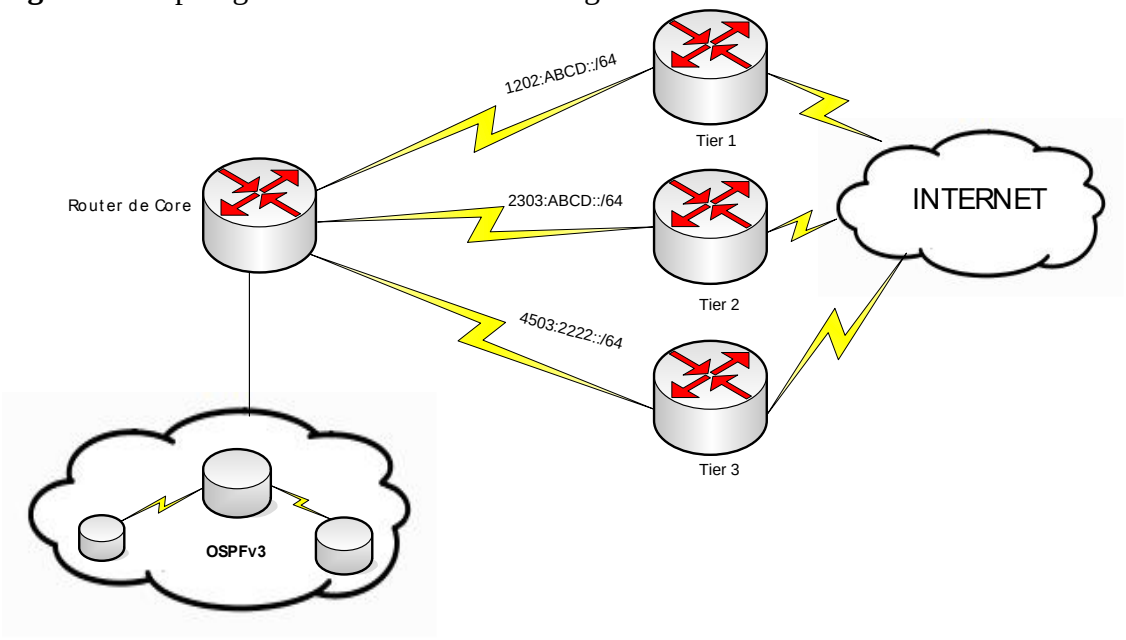
Router	**IP**	**Tipo de Dirección**	**INT**
MTZ_UIO	2004:BF9:0:5::1	GLOBAL-UNICAST	fa0/0
Sucumbíos	2004:BF9:0:5::2		
RED	**Prefijo**	**Rango**	
2004:bf9:0:5::	/64	**Desde**	**Hasta**
		2004:0bf9:0000:0005::	2004:0bf9:0000:0005:ffff:ffff:ffff:ffff

Elaborado por: Fausto Flores

3.1.3 Topología BGP – Multihoming

Para la topología BGP-4 con IPv6 se cuenta con 3 salidas internacionales. Los tres proveedores se denominan: Tier1, Tier2 y Tier3. Estos brindan redundancia a la red en caso de que uno o dos enlaces fallen.

Figura 13 Topología BGP-4 con Multihoming



Elaborado por: Fausto Flores

En la figura 13 , se puede verificar que el ISP se conecta por medio del router de core a las 3 salidas internacionales (Tier1, Tier2 y Tier3), brindando un valor agregado a los usuarios ya que si se pierde la conexión del enlace principal, el enlace de respaldo entra a funcionar.

Para la emulación de BGP-4 con Multihoming sobre IPv6 de ha utilizado las siguientes características y herramientas:

- Conexión desde el ISP hacia los 3 proveedores de servicio de Internet.
- Imagen de IOS cisco con versión 12.4 y soporte BGP-4 e IPv6. Para esta emulación se ha usado un Router Cisco 7200 ya que cumple con las características necesarias.

La tabla 12, hace referencia al direccionamiento IPv6, correspondiente al router de core y su conexión con el router correspondiente al Tier1.

Tabla 12 Direccionamiento IPv6 Core-Tier 1

Router	IP	Tipo de Dirección	INT
Core	2001:ABCD::21B:54FF:FEA9:24B1	RESERVED	fa0/0
Tier 1	2001:ABCD::21B:54FF:FEA9:24B2		fa0/0
RED	**PREFIJO**	**Rango**	
2001:ABCD::	/64	**Desde**	**Hasta**
	/64	2001:abcd::	2001:abcd:0000:0000:ffff:ffff:ffff:ffff

Elaborado por: Fausto Flores

La tabla 13, hace referencia al direccionamiento IPv6, correspondiente al router de core y su conexión con el router correspondiente al Tier2.

Tabla 13 Direccionamiento IPv6 Core-Tier 2

Router	IP	Tipo de Dirección	INT
Core	fa0/1	RESERVED	2002:ABCD::21B:54FF:FE54:FB11
Tier 2	fa0/1		2002:ABCD::21B:54FF:FE54:FB12
RED	**Prefijo**	**Rango**	
2002:ABCD::	/64	**Desde**	**Hasta**
	/64	2002:abcd::	2002:abcd:0000:0000:ffff:ffff:ffff:ffff

Elaborado por: Fausto Flores

La tabla 14, hace referencia al direccionamiento IPv6, correspondiente al router de core y su conexión con el router correspondiente a Tier3.

Tabla 14 Direccionamiento IPv6 Core-Tier 3

Router	IP	Tipo de Dirección	INT
Core	2001:2222::21B:54FF:FE54:F111	RESERVED	fa2/1
Tiert 3	2001:2222::21B:54FF:FE54:F112		fa2/1
RED	**Prefijo**	**Rango**	
2001:2222::	/64	**Desde**	**Hasta**
	/64	2001:2222::	2001:2222:0000:0000:ffff:ffff:ffff:ffff

Elaborado por: Fausto Flores

3.2 Configuración del escenario de simulación: instalación y configuración de gns3, VMWare 9 y sistemas operativos

3.2.1 Instalación de gns3 y cisco IOS

GNS3 es un software multiplataforma, además de ser muy beneficioso, ya que se ajusta perfectamente con Wireshark, Qemu e inclusive si se dispone varias tarjetas de red. Se puede emular una red a partir de estas y evaluar cómo se comportaría el modelo del router dentro de una topología y con una configuración determinada.

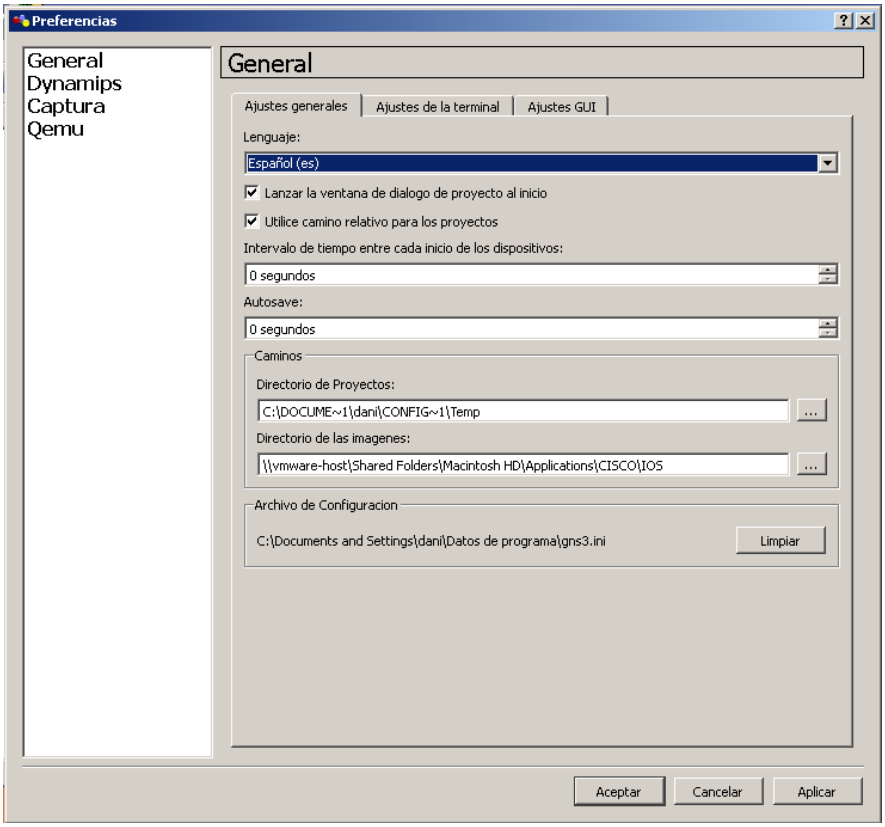
Instalación en Windows 7

La descarga de GNS3, se puede realizar del siguiente link http: //www.gns3.net/download/, dentro del paquete se encuentra Dynamips, Putty, WinPCAP y Quemu/Pemu.

El proceso de instalación es sencillo, como la mayoría de las instalaciones en Windows se hace un next a todo lo solicitado luego de ejecutar el instalador.

Una vez completado los pasos anteriores, solo queda seleccionar las imágenes IOS que se va a utilizar; desde la carpeta elegida en el paso anterior, para esto se siguen los siguientes pasos: en el menú Editar -> Imágenes IOS y hypervisors. En la pestaña Imagen, seleccionar los IOS a utilizar. Opcional configurar algunos datos como el modelo del IOS, la RAM y otras opciones más.

Figura 14 Preferencias de GNS3



Elaborado por: Fausto Flores

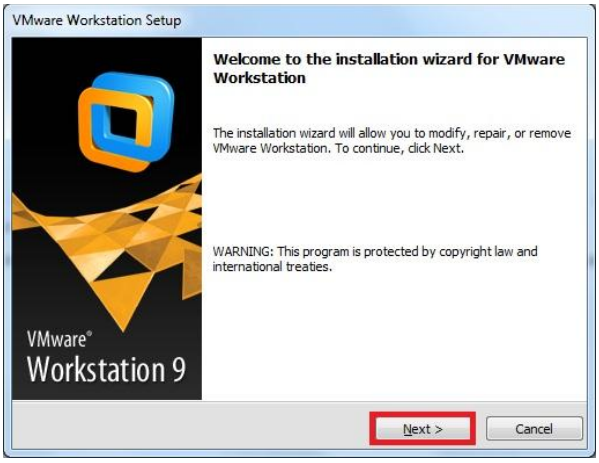
Como último paso se debe probar si el módulo Dynamips funciona correctamente, para esto ir al menú Editar -> Preferencias -> Dynamips -> clic en el botón Test. Si se consigue un mensaje en color verde, se puede empezar a utilizar GNS3 en Windows 7.

3.2.2 Instalación de VMWare y Centos 6.3

La descarga de VMWare, se puede realizar del siguiente link https://my.vmware.com/web/vmware/downloads

Una vez descargado se ejecuta el instalador

Figura 15 Ventana de bienvenida

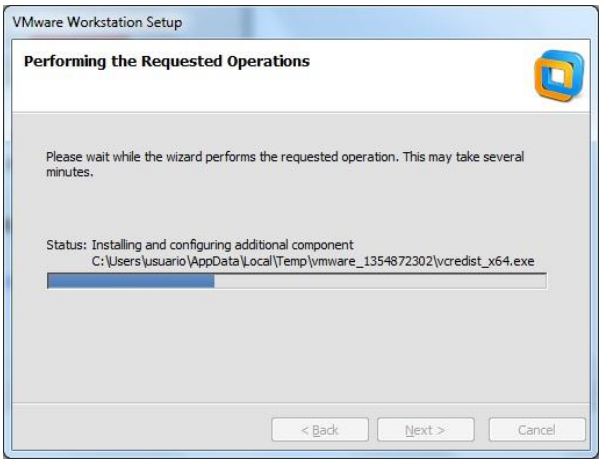


Elaborado por: Fausto Flores

Se pulsa **Next**, como en la figura 15. Aparece el tipo de instalación como se referencia en la figura 17, a continuación clic en next.

Luego, aparecerá una serie de ventanas previas para completar la instalación, y se configure una serie de características propias del programa como: updates, ayuda, accesos directos y una ventana final de confirmación previa a la instalación.
En la figura 16 se ha capturado el proceso de instalación de VMWare.

Figura 16 Proceso de instalación de VMWare



Elaborado por: Fausto Flores

Una vez completo el proceso de instalación dar clic en el botón finish y se tiene el programa instalado en el equipo.

3.3 Configuraciones de los equipos

3.3.1 Configuración: red de área local LAN

3.3.1.1 Configuración del direccionamiento ipv6 en el servidor

Para poner el servidor en funcionamiento se requiere realizar una configuración inicial en la cual se toma en cuenta los siguientes parámetros:

Configuración IPv6

Centos por default no permite al usuario Root iniciar la sesión, por lo cual es necesario autenticarse con el usuario creado al momento de la instalación.

Abrir una consola y autenticarse como súper usurario.

```
# su – “autenticarse como super usario””
```

Sin embargo, si se requiere mantener esta configuración después de un reinicio. Se debe seguir los siguientes pasos:

Figura 17 Configuración de IPv6 en Centos 6.4

```
[root@localhost ~]# vi /etc/sysconfig/network “Archivo de configuración de red”
NETWORKING=yes
HOSTNAME=servidor
NETWORKING_IPV6=yes “Activa IPv6”
:wq “Guarda y abandona el editor vi”
```

Elaborado por: Fausto Flores

En la figura 18 se describe la configuración de la interfaz Ethernet 0.

Figura 18 Configuración de la interfaz en el servidor

```
[root@localhost ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
BOOTPROTO="static" “Refiere a una configuración manual”
ONBOOT="yes" “Refiere inicio de la interfaz cada reinicio del S.O”
HWADDR="2C:C3:AC:A8:C3:3E" “MAC address”
#IPADDR= N/A “Dirección IPv4”
#GATEWAY= N/A
#NETMASK= N/A
TYPE=Ethernet
IPV6INIT=yes “Activa IPv6”
IPV6ADDR=2001:FBC:DA42:3::2/64 “Dirección IPv6”
IPV6_DEFAULTGW=2001:FBC:DA42:3::1

#DNS1=N/A
#DNS2=N/A
# Only DNS{1,2} according to /usr/share/doc/initscripts-9.03.27/sysconfig.txt
#DNS3=2620:0:ccc::2
#DNS4=2620:0:ccD::2
```

Elaborado por: Fausto Flores

En la figura 19 se describe el paso para el reinicio de la interfaz Eth0.

Figura 19 Reiniciar de la red para que los cambios tengan efecto

```
[root@localhost ~]# service network restart
Shutting down interface Auto_eth0:  Device state: 3 (disconnected)
                                                           [  OK  ]
Shutting down interface eth0:                               [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface Auto_eth0:  Active connection state: activating
Active connection path: /org/freedesktop/NetworkManager/ActiveConnection/2
state: activated
Connection activated
                                                           [  OK  ]
                                                           [  OK  ]
```

Elaborado por: Fausto Flores

Como se puede verificar en la configuración anterior los servicios de red se han levantado sin problemas luego de aplicar la configuración IPv6, con este precedente se puede continuar con la configuración de los servicios HTTP, SMTP y FTP.

3.3.1.2 Configuración de Servicios: HTTP, SMTP y FTP sobre IPv6

Configuración HTTP en IPv6

Antes de iniciar la configuración del servicio, comprobar la versión que tiene instalada de Apache con el fin de realizar una actualización por cuestiones de seguridad, para este caso no es necesario.

Figura 20 Versión de Apache

```
[root@localhost ~]# httpd -v
Server version: Apache/2.2.15 (Unix)
Server built:   Aug 13 2013 17:27:11
```

Elaborado por: Fausto Flores

En la figura 21 se describe la configuración del archivo del servidor Apache mediante el editor vi con el fin de activar el soporte de IPv6.

Figura 21 Archivo httpd.conf

```
[root@localhost ~]# cd /etc/httpd/conf/
[root@localhost conf]# ls
httpd.conf  magic
[root@localhost conf]# vi httpd.conf
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, in addition to the default. See also the <VirtualHost>
# directive.
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#Listen 12.34.56.78:80// Comentar listen para IPv4
Listen 80 “Para el caso de estudio se considera la publicación del servicio a
cualquier IPv6”
#Listen [2001:ABC:FD53:4::/64]:80 //Agregar direcciones IPv6 confiables
#Listen [2001:FBC:DA42:3::2]:80
:wq //Guarda y abandona el editor vi
```

Elaborado por: Fausto Flores

Reiniciar el servicio con el fin de cargar la nueva configuración y verificar que el puerto 80 se encuentre abierto para IPv6.

Figura 22 Reinicio del servicio httpd

```
[root@localhost /]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
[root@localhost /]# netstat -tulpn | grep :80
tcp        0      0 :::80                       :::*                        LISTEN
6375/httpd
```

Elaborado por: Fausto Flores

Las configuraciones que ip6tables trae por defecto, bloquea el puerto 80 para el tráfico que proviene de cualquier red hacia el servidor es decir los datos de entrada. Por lo cual se requiere realizar la siguiente modificación en el archivo ip6tables-config, el cual se encuentra dentro de la ruta /etc/sysconfig/.

Figura 23 Apertura de Puerto HTTP en IPv6

```
root@localhost sysconfig]# ls
atd            i18n              network-scripts  selinux
auditd         init              nspluginwrapper  sendmail
authconfig     ip6tables-config  ntpd             smartmontools
cbq            ip6tables.old     ntpdate          snmpd
cpuspeed       irqbalance        raid-check       sysstat
crond          kdump             readahead        sysstat.ioconf
root@localhost sysconfig]# vi /etc/sysconfig/ip6tables
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 80 -j ACCEPT //En la política de Input
se abre el puerto 80 para el protocolo tcp.

Añadir el siguiente si ha configurado el puerto HTTPS:

-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 443 -j ACCEPT // En la política de
Input se abre el puerto 433 para el protocolo tcp.

:wq “Guarda y abandona el editor vi”
```

Elaborado por: Fausto Flores

Una vez realizado los cambios, Reiniciar el servicio de Ip6tables

```
[root@localhost sysconfig]# service ip6tables restart
```

Configuración SMTP en IPv6

Antes de iniciar la configuración del servicio, comprobar la versión de Sendmail que se tiene instalada con el fin de realizar una actualización por cuestiones de seguridad en el caso de ser necesario, para este caso no aplica.

Figura 24 Versión de Apache

```
[root@localhost ~]# httpd -v
Server version: Apache/2.2.15 (Unix)
Server built:   Aug 13 2013 17:27:11
```

Elaborado por: Fausto Flores

Ingresar al archivo de configuración mediante el editor vi:

Para habilitar IPv6 en Sendmail y configurar el servidor, primero se debe editar el fichero sendmail.mc, de la siguiente manera:

Figura 25 Configuración del archivo sendmail.mc

```
DAEMON_OPTIONS (`port=smtp, Name=MTA, Family=inet6')dnl // Activa el protocol uso
del protocol IPv6 para Mail transfer Agent
DAEMON_OPTIONS(`port=smtp,Addr=2001:FBC:DA42:3::2, Name=MTA-v6, Family=inet6')dn
L //// Activa el uso protocol del protocol IPv6 para Mail transfer Agent y la
asocial con la dirección del servidor.
Dnl DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl //linea comentada
FEATURE(`accept_unresolvable_domains')dnl// se activa la recepción de correos para
dominios que el DNS no resuelve.
LOCAL_DOMAIN(`localhost.localdomain')dnl // Activa la recepción de correos locales
MASQUERADE_AS(`mail.ups.ec')dnl // Activa la recepción de correos del dominio
mail.ups.ec
MASQUERADE_DOMAIN(mail.ups.ec)dnl
MAILER(smtp)dnl // configura como protocolo de transferencia de correos a SMTP
dnlMAILER(procmail)dnl // Se desactiva el uso de procmail
dnl MAILER(cyrusv2)dnl // Se desactiva el uso de cyrusv2
```

Elaborado por: Fausto Flores

A continuación, hay que reconstruir la configuración y reiniciar Sendmail, para esto se utiliza el siguiente comando:

Figura 26 Compilación del archive sendmail.rc

```
make -C /etc/mail
service sendmail restart
```

Elaborado por: Fausto Flores

El siguiente paso en la configuración es ingresar y editar el archivo local-host-names, para incluir el dominio al cual está unido el servidor de correos:

Figura 27 Dominios administrador por SMTP

```
vi /etc/mail/local-host-names
dominio1.com
dominio2.com.ec
dominio3.org
:Wq //guardar y salir
```

Elaborado por: Fausto Flores

Se debe crear el archivo relay-domains con el fin de agregar los dominios que tendrán permitido la re-transmisión del correo electrónico dentro del servidor:

Figura 28 Dominios de re-transmisión

```
vi /etc/mail/relay-domains
dominio1.com
dominio2.com.ec
dominio3.org
:Wq //guardar y salir
```

Elaborado por: Fausto Flores

Las listas de control de acceso se utiliza para definir los dominios o IP's que pueden enviar correos utilizando el servidor, para esto se debe editar las listas de control de acceso, en el archivo /etc/mail/access:

Figura 29 Listas de control acceso

```
vi /etc/mail/access
Connect:localhost.localdomain        RELAY
Connect:localhost           RELAY
Connect:127.0.0.1           RELAY
#
# Dirección IP del propio servidor.
Connect:2001:FBC:DA42:3::2/64        RELAY
#
# Otros servidores de correo en la LAN a los que se les permitirá enviar
# correo libremente a través del propio servidor de correo.
Connect:                    RELAY
#
#
# Lista negra
usuario@noPermitido.com     REJECT
spam.com.mx                 REJECT
2002:ADF:CB42:3:: /64       REJECT
```

Elaborado por: Fausto Flores

Configuración FTP en IPv6

Antes de iniciar la configuración del servicio, comprobar la versión de VSFTPd que se tiene instalada con el fin de realizar una actualización por cuestiones de seguridad en el caso de ser necesario, para este caso la más reciente actualización está instalada en el servidor.

Figura 30 Versión de vsftpd

```
[root@localhost ~]# rpm -qa | grep vsftpd
vsftpd-2.2.2-11.el6_4.1.i686
```

Elaborado por: Fausto Flores

A continuación se agrega un usuario vsftpd :

Figura 31 Usuario vsftpd

```
useradd ftpuser
passwd ftpuser
```

Elaborado por: Fausto Flores

Ingresar al archivo de configuración mediante el editor vi:

Figura 32 Configuración de vsftpd

```
vi /etc/vsftpd/vsftpd.conf
# Example config file /etc/vsftpd/vsftpd.conf
#
# permitir usuario anónimo FTP? (Tener Cuidado - permitido por defecto si comenta
esto).
anonymous_enable=YES
#
# Elimine esta opción para permitir a usuarios locales inician sesión.
local_enable=YES
#
# Descomentar esta opción para que cualquier tipo de comando de escritura de FTP.
write_enable=YES
#
#Descomente esta opción para permitir que el usuario FTP anónimo pueda subir
archivos. Esto #sólo tiene efecto si la escritura global está activada.
#anon_upload_enable=YES
#
# asegura que las conexiones de transporte al puerto origen, en el puerto 20 (ftp-
data).
connect_from_port_20=YES
#
# Puede personalizar completamente el mensaje de inicio de sesión:
#ftpd_banner=Bienvenido a la session FTP.
#
# Se puede especificar una lista explícita de los usuarios locales en el archivo
chroot(). Si chroot_local_user tiene un valor de YES, entonces se tendrá acceso al
servidor.

chroot_list_enable=YES
# se tiene por defecto la siguiente dirección.
chroot_list_file=/etc/vsftpd/chroot_list
#
# esta opción permite ejecutar de modo independiente sockets IPv4. Nota: Esta
directriz no se puede utilizar en combinación con la directriz #listen_ipv6.
listen=NO
#
# Esta directiva permite la escucha en sockets IPv6. Para escuchar en IPv4 y
sockets IPv6, debe ejecutar dos copias de un poco con dos archivos de configuración
de vsftpd. Asegúrese de que una de las opciones que se escuchan comentarios!
listen_ipv6=YES
```

Elaborado por: Fausto Flores

Guardar los cambios y reiniciar el servidor.

3.3.1.3 Configuración LAN para routers Cisco

Para el enrutamiento en la parte LAN, se tiene un ruteo estático ya que el servidor se encuentra conectado a un solo enlace, es decir la puerta de salida de la información es la misma.

El modelo del router es cisco 7200, Para el segmento de LAN, el equipo representa el concentrador de los datos a nivel provincial.

Dentro de la configuración se encuentran las siguientes características:

Router de datos Loja:

Paso 1: Configuración general del equipo. En la tabla 15 se realiza una descripción de los comandos utilizados para la configuración general de los equipos.

Tabla 15 Descripción de línea de comandos, configuración básica

Comando	Descripción
Loja>enable	Permite ingresar al modo de configuración global y usar los comandos generales del router.
Loja(config)#hostname nombre	Permite agregar un nombre al router
Loja(config)#enable secret clave	Permite poner una clave de acceso al modo de configuración global
Loja(config)#line vty 0 Loja(config-line)#password clave Loja(config-line)#login	Establecer una clave para el acceso remoto al router.
Loja(config)#line con 0 Loja(config-line)#password clave Loja(config-line)#login	Establecer una clave de acceso para la conexión al puerto de consola.
Loja#Write	Realiza una copia de la información.
Loja(config)# line console	Entra a la configuración de la línea de consolas
Loja(config-console)# exec-timeout 0 0	Establece el tiempo en que la sesión expira, para el caso esta opción está desactivada
Loja(config)#privilege level 15	Establece el nivel de privilegio para los comandos de cisco, en este caso se tiene todos los privilegios
Loja(config)# line aux 0	Entra a la configuración de la línea auxiliar

Elaborado por: Fausto Flores

Router Loja LAN:

Mediante el comando s*how run* se verifica la configuración básica aplicada al router de Loja.

Figura 33 Configuración del router de Loja

```
Loja#sh run
Building configuration...

Current configuration : 1414 bytes
!
version 12.4
hostname Loja
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password clave
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
¡
end
```

Elaborado por: Fausto Flores

Router Sucumbios LAN:

Mediante el comando s*how run* se verifica la configuración básica aplicada al router de Sucumbios.

Figura 34 Configuración del router de Sucumbios

```
Sucumbios#sh run
Building configuration...

Current configuration : 1414 bytes
!
version 12.4
hostname Sucumbios
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password clave
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
¡
end
```

Elaborado por: Fausto Flores

Paso 2: Configuración IPv6 del equipo. En la tabla 16 se realiza una descripción de los comandos utilizados para la configuración IPv6 del equipo.

Tabla 16 Descripción de línea de comandos, configuración IPv6

Comando	Descripción
Loja(config)#**ipv6 unicast-routing**	Una dirección unicast IPv6 es un identificador para una única interfaz, en un solo nodo. Un paquete que se envía a una dirección unicast se entrega a la interfaz identificada por dicha dirección. El comando habilita dicha característica.
Loja(config)#**interface** fastEthernet 0/1	Permite ingresar a la configuración específica de la interfaz
Loja(config-if)#**no shutdown**	Habilita la interfaz físicamente para la comunicación con otros dispositivos.
Loja(config-if)# **ipv6 enable**	Habilita el protocolo IPv6.
Loja(config-if)#**ipv6 address** 2003:AC9:0:4::2/64	Asignación a la interfaz la dirección IPv6.
Loja(config-if)#**speed auto**	La velocidad de configuración se ajusta al del router vecino conectado a la interfaz.

Elaborado por: Fausto Flores

Configuración IPv6 router Loja LAN:

Mediante el comando s*how run* se verifica la configuración IPv6 aplicada al router de Loja.

Figura 35 Configuración IPv6 router Loja

```
Loja#sh run
Building configuration...
interface FastEthernet0/0
 description MTZ_GYE
 no ip address
 duplex auto
 speed auto
 ipv6 address 2003:AC9:0:4::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:FBC:DA42:3::1/64
 ipv6 enable
end
```

Elaborado por: Fausto Flores

Configuración IPv6 router Sucumbíos LAN:

Mediante el comando s*how run* se verifica la configuración IPv6 aplicada al router de Sucumbíos.

Figura 36 Configuración IPv6 router Sucumbíos

```
Sucumbios#sh run
Building configuration...
ipv6 unicast-routing
interface FastEthernet0/0
 description to MTZ_Quito
 no ip address
 duplex auto
 speed auto
 ipv6 address 2004:BF9:0:5::2/64
 ipv6 ospf 1 area 0
!
end
```

Elaborado por: Fausto Flores

3.3.2 Configuración Open Shortest Path First OSPFv3 para routers Cisco

Paso 1: Configuración general del equipo. En la tabla 17 se realiza una descripción de los comandos utilizados para la configuración general de los equipos.

Tabla 17 Descripción de línea de comandos, configuración básica

Comando	**Descripción**
Router>**enable**	Ingresa al modo de configuración global y usa los comandos generales del router.
Router(config)#hostname nombre	Agregar un nombre al router
Router(config)#enable secret clave	Permite poner una clave de acceso al modo de configuración global
Router(config)#line vty 0 Router(config-line)#password clave Router(config-line)#login	Establecer una clave para el acceso remoto al router.
Router(config)#line con 0 **Router(config-line)#password clave** **Router(config-line)#login**	Establecer una clave de acceso para la conexión al puerto de consola.
Router#Write	Realiza una copia de la información. Para el uso del comando se debe estar en el modo de configuración global.

Elaborado por: Fausto Flores

Configuración Básica Router Core:

Mediante el comando s*how run* se verifica la configuración básica aplicada al router de Core.

Figura 37 Configuración básica router Core

```
Core#sh run
Building configuration...

Current configuration : 2591 bytes
!
version Core
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password clave
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end
```

Elaborado por: Fausto Flores

Nota: La configuración es estándar para los siguientes equipos que participan en el dominio OSPFv3.

Paso 2: Configuración IPv6 de los equipos que componen el dominio OSPFv3. En la tabla 18 se realiza una descripción de los comandos utilizados para la configuración IPv6 de los equipos.

Tabla 18 Descripción de línea de comandos, configuración IPv6

Comando	Descripción
Router(config)#ipv6 unicast-routing	Una dirección unicast IPv6 es un identificador para una única interfaz, en un solo nodo. Un paquete que se envía a una dirección unicast se entrega a la interfaz identificada por dicha dirección. El comando habilita dicha característica.
Router(config)#interface fastEthernet 0/1	Ingresar a la configuración específica de la interfaz
Router(config-if)#no shutdown	Habilita la interfaz físicamente para la comunicación con otros dispositivos.
Router(config-if)# ipv6 enable	Habilita el protocolo IPv6.
Router(config-if)#ipv6 address x:x:x:x:x:x:x/64	Asignación a la interfaz la dirección IPv6.
Router(config-if)#speed auto	La velocidad de configuración se ajusta al del router vecino conectado a la interfaz.

Elaborado por: Fausto Flores

Configuración IPv6 Router Core:

Mediante el comando s*how run* se verifica la configuración IPv6 aplicada al router de Core.

Figura 38 Configuración IPv6 router de Core

```
CORE#sh run
Building configuration...
Current configuration : 2591 bytes
!
version 12.4
ipv6 unicast-routing
ipv6 cef
!
interface FastEthernet0/0
 description To_Tier_1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:ABCD::21B:54FF:FEA9:24B1/64
 ipv6 enable
!
interface FastEthernet0/1
 description To_Tier_2
 no ip address
 duplex auto
 speed auto
 ipv6 address 2002:ABCD::21B:54FF:FE54:FB11/64
 ipv6 enable
!
interface FastEthernet1/0
 description To_MTZ_Quito
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:0:1::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet2/0
 description To_MTZ_GYE
 no ip address
 duplex auto
 speed auto
 ipv6 address 2002:ADB8:0:3::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet2/1
 description To_Tier_3
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:2222::21B:54FF:FE54:F111/64
 ipv6 enable
end
```

Elaborado por: Fausto Flores

Configuración IPv6 Router Matriz Quito:

Mediante el comando s*how run* se verifica la configuración IPv6 aplicada al router de MTZ_Quito.

Figura 39 Configuración IPv6 router Matriz Quito

```
MTZ_Quito#sh run
Building configuration...
Current configuration : 1387 bytes
interface FastEthernet0/0
 description To_Sucumbios
 no ip address
 duplex auto
 speed auto
 ipv6 address 2004:BF9:0:5::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
interface FastEthernet1/0
 description To_Core
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:0:1::2/64
ipv6 enable
 ipv6 ospf 1 area 0
end
```

Elaborado por: Fausto Flores

Configuración IPv6 Router Matriz Guayaquil:

Mediante el comando s*how run* se verifica la configuración IPv6 aplicada al router de MTZ_GYE.

Figura 40 Configuración IPv6 router Matriz Guayaquil

```
MTZ_GYE#sh run
Building configuration...
Current configuration : 1349 bytes
ipv6 unicast-routing
interface FastEthernet0/0
 description to_Loja
 no ip address
 duplex auto
 speed auto
 ipv6 address 2003:AC9:0:4::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet2/0
 description To_Core
 no ip address
 duplex auto
 speed auto
 ipv6 address 2002:ADB8:0:3::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
end
```

Elaborado por: Fausto Flores

Paso 3: Configuración de enrutamiento OSPFv3. En la tabla 19 se realiza una descripción de los comandos utilizados para la configuración de OSPFv3 en los equipos.

Tabla 19 Descripción de línea de comandos, configuración OSPFv3

Comando	Descripción
Loja(config)# **ipv6 router ospf** 1	Para habilitar Open Shortest Path First (OSPF) en el modo de configuración del router IPv6, utilizar el comando en modo de configuración global.
Loja(config-rtr)#**router-id** 3.3.3.3	Por defecto, cuando se inicia el proceso de OSPF, selecciona la dirección IP más alta en un router como el ID del router en el proceso de OSPF. El ID del router identifica de forma exclusiva un router dentro de un dominio OSPF. El comando se utiliza para definir de forma manual el identificador del router.
Loja(config-rtr)#log-adjacency-changes	Muestra en consola si existe algún cambio o mensaje dentro de la topología OSPF
Loja(config-rtr)#**redistribute connected**	Distribuye las direcciones que se encuentran directamente conectadas al router.
Loja(config-rtr)#**redistribute static**	Distribuye las rutas estáticas configuradas en el router.
Loja(config-rtr)# **ipv6 ospf** 1 **area** 0	Agrega al area 0 el proceso OSPF configurado.

Elaborado por: Fausto Flores

Tabla 20 Direccionamiento OSPFv6

Router	IP	Interface	OSPFv6 Área	Router-id
Sucumbíos	2001:BF9:0:5::2	fa0/0	Área 0	2.2.3.2
MTZ_Quito hacia Sucumbíos	2001:BF9:0:5::1	fa0/0	Área 0	2.2.3.1
Loja	2001:AC9:0:4::2	fa0/0	Area 0	3.3.4.2
MTZ_Guayaquil hacia Loja	2001:AC9:0:4::1	fa0/0	Area 0	3.3.4.1
MTZ_Quito hacia Core	2001:DB8:0:1::2	fa1/0	Area 0	2.2.3.1
Core hacia MTZ_Quito	2001:DB8:0:1::1	fa1/0	Area 0	3.3.4.3
Core hacia MTZ_Guayaquil	2002:ADB8:0:3::1	fa2/0	Area 0	3.3.4.3
MTZ_Guayaquil hacia Core	2002:ADB8:0:3::2	fa2/0	Area 0	3.3.4.1

Elaborado por: Fausto Flores

En la tabla 20 se detalla el direccionamiento IPv6 utilizado en las configuraciones del enrutamiento de OSPFv6 así como el identificador de cada router. El Rouder-id sirve para identificar al router dentro del sistema autónomo.

Configuración OSPFv3 Router Core:

Mediante el comando s*how run* se verifica la configuración OSPFv3 aplicada al router de CORE.

Figura 41 Configuración OSPFv3 Router Core

```
CORE#sh run
Building configuration...
interface FastEthernet1/0
 description To_MTZ_Quito
ipv6 ospf 1 area 0
!
interface FastEthernet2/0
 description To_MTZ_GYE
!
ipv6 ospf 1 area 0
router bgp 100
address-family ipv6
redistribute ospf 1
!
ipv6 router ospf 1
 router-id 3.3.4.3
 log-adjacency-changes
 redistribute connected
 redistribute static
 redistribute bgp 100
end
```

Elaborado por: Fausto Flores

Configuración OSPFv3 Router Matriz Quito:

Mediante el comando s*how run* se verifica la configuración OSPFv3 aplicada al router de MTZ_Quito.

Figura 42 Configuración OSPFv3 Router Matriz Quito

```
MTZ_Quito#sh run
Building configuration...
!
interface FastEthernet0/0
  ipv6 ospf 1 area 0
!
interface FastEthernet1/0
  ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 2.2.3.1
 log-adjacency-changes
end
```

Elaborado por: Fausto Flores

Configuración OSPFv3 Router Matriz Guayaquil:

Mediante el comando s*how run* se verifica la configuración OSPFv3 aplicada al router de MTZ_GYE.

Figura 43 Configuración OSPFv3 Router Matriz Guayaquil

```
MTZ_GYE#sh run
Building configuration...
!
interface FastEthernet0/0
ipv6 ospf 1 area 0
!
interface FastEthernet2/0
  ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 3.3.4.1
 log-adjacency-changes
end
```

Elaborado por: Fausto Flores

Configuración OSPFv3 Router Sucumbíos:

Mediante el comando s*how run* se verifica la configuración OSPFv3 aplicada al router de Sucumbíos.

Figura 44 Configuración OSPFv3 Router Sucumbíos

```
Sucumbios#sh run
interface FastEthernet0/0
 description to MTZ_Quito
!
ipv6 ospf 1 area 0
ipv6 router ospf 1
 router-id 2.2.3.2
 log-adjacency-changes
!
end
```

Elaborado por: Fausto Flores

Configuración OSPFv3 Router Loja:

Mediante el comando s*how run* se verifica la configuración OSPFv3 aplicada al router de Loja.

Figura 45 Configuración OSPFv3 Router Loja

```
Loja#sh run
!
interface FastEthernet0/0
  ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 3.3.4.2
 log-adjacency-changes
 redistribute connected
 redistribute static
!
end
```

Elaborado por: Fausto Flores

3.3.3 Configuración: Boarder Gateway Protocol BGP – Multihoming

Paso 1: Configuración general del equipo. En la tabla 21 se realiza una descripción de los comandos utilizados para la configuración general de los equipos.

Tabla 21 Descripción de línea de comandos, configuración básica equipos BGP

Comando	Descripción
Router>**enable**	Permite ingresar al modo de configuración global y usar los comandos generales del router.
Router(config)#hostname nombre	Permite agregar un nombre al router
Router(config)#enable secret clave	Permite poner una clave de acceso al modo de configuración global
Router(config)#line vty 0 Router(config-line)#password clave Router(config-line)#login	Establecer una clave para el acceso remoto al router.
Router(config)#line con 0 **Router(config-line)#password clave** **Router(config-line)#login**	Establecer una clave de acceso para la conexión al puerto de consola.
Router#Write	Realiza una copia de la información. Para el uso del comando se debe estar en el modo de configuración global.

Elaborado por: Fausto Flores

Configuración Básica Router Tier_1:

Mediante el comando s*how run* se verifica la configuración básica aplicada al router Tier_1.

Figura 46 Configuración Básica Router Tier_1

```
Tier_1#sh run
Building configuration...

Current configuration : 2002 bytes
!
Hostname Tier_1
version Core
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password clave
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
¡
end
```

Elaborado por: Fausto Flores

Nota: La configuración básica es estándar para todos los equipos que participan en el dominio BGP-4.

Paso 2: Configuración IPv6 de los equipos que participan en el dominio BGP-4. En la tabla 22 se realiza una descripción de los comandos utilizados para la configuración IPv6 de los equipos.

Tabla 22 Descripción de línea de comandos, configuración IPv6

Comando	Descripción
Router (config)#ipv6 unicast-routing	Una dirección unicast IPv6 es un identificador para una única interfaz, en un solo nodo. Un paquete que se envía a una dirección unicast se entrega a la interfaz identificada por dicha dirección. El comando habilita dicha característica.
Router (config)#interface fastEthernet 0/1	Permite ingresar a la configuración específica de la interfaz
Router (config-if)#no shutdown	Habilita la interfaz físicamente para la comunicación con otros dispositivos.
Router (config-if)# ipv6 enable	Habilita el protocolo IPv6.
Router (config-if)#ipv6 address x:x:x:x:x:x:x/64	Asignación a la interfaz la dirección IPv6.
Router (config-if)#speed auto	La velocidad de configuración se ajusta al del router vecino conectado a la interfaz.

Elaborado por: Fausto Flores

Tabla 23 Direccionamiento BGP-4

Router	IP	Interface	AS	Router-id
Core hacia Tier 1	2001:ABCD::21B:54FF:FEA9:24B1	fa0/0	100	1.1.1.1
Tier 1 hacia Core	2001:ABCD::21B:54FF:FEA9:24B2	fa0/0	200	2.2.2.2
Core hacia Tier 2	2002:ABCD::21B:54FF:FE54:FB11	fa0/1	100	1.1.1.1
Tier 2 hacia Core	2002:ABCD::21B:54FF:FE54:FB12	fa0/1	300	3.3.3.3
Core hacia Tier 3	2001:2222::21B:54FF:FE54:F111	fa2/1	100	1.1.1.1
Tiert 3 hacia Core	2001:2222::21B:54FF:FE54:F112	fa2/1	400	4.4.4.4

Elaborado por: Fausto Flores

En la tabla 23 se detalla el direccionamiento IPv6 utilizado en las configuraciones del enrutamiento de BGP-4 así como el identificador de cada router. El Rouder-id sirve para identificar al router dentro del dominio de BGP así como el sistema autónomo, cabe indicar que estos atributos son únicos para cada dispositivo.

Configuración IPv6 Router Core:

Mediante el comando s*how run* se verifica la configuración IPv6 aplicada al router CORE referente a BGP-4.

Figura 47 Configuración IPv6 Router Core

```
CORE#sh run
interface FastEthernet0/0
 description To_Tier_1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:ABCD::21B:54FF:FEA9:24B1/64
 ipv6 enable
!
interface FastEthernet0/1
 description To_Tier_2
 no ip address
 duplex auto
 speed auto
 ipv6 address 2002:ABCD::21B:54FF:FE54:FB11/64
 ipv6 enable
!
interface FastEthernet1/0
 description To_MTZ_Quito
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:0:1::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet2/0
 description To_MTZ_GYE
 no ip address
 duplex auto
 speed auto
 ipv6 address 2002:ADB8:0:3::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet2/1
 description To_Tier_3
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:2222::21B:54FF:FE54:F111/64
 ipv6 enable
end
```

Elaborado por: Fausto Flores

Configuración IPv6 Router Tier_1:

Mediante el comando s*how run* se verifica la configuración IPv6 aplicada al router Tier_1 referente a BGP-4.

Figura 48 Configuración IPv6 Router Tier_1

```
Tier_1#sh run
ipv6 unicast-routing
!
interface FastEthernet0/0
 description To_ISP_Core
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:ABCD::21B:54FF:FEA9:24B2/64
 ipv6 enable
!
interface FastEthernet2/0
 description To_Tier_4
 no ip address
 duplex auto
 speed auto
 ipv6 address 8502:3333::21B:54AB:FE54:A211/64
 ipv6 enable
end
```

Elaborado por: Fausto Flores

Configuración IPv6 Router Tier_2:

Mediante el comando s*how run* se verifica la configuración IPv6 aplicada al router Tier_2 referente a BGP-4.

Figura 49 Configuración IPv6 Router Tier_2

```
Tier_2#sh run
ipv6 unicast-routing
!
interface FastEthernet0/1
 description To_ISP_Core
 no ip address
 duplex auto
 speed auto
 ipv6 address 2002:ABCD::21B:54FF:FE54:FB12/64
 ipv6 enable
!
interface FastEthernet2/1
 description To_ISP_B
 no ip address
 duplex auto
 speed auto
 ipv6 address 5602:5555::72A:65CC:CA55:A621/64
 ipv6 enable
!
end
```

Elaborado por: Fausto Flores

Configuración IPv6 Router Tier_3:

Mediante el comando s*how run* se verifica la configuración IPv6 aplicada al router Tier_3 referente a BGP-4.

Figura 50 Configuración IPv6 Router Tier_3

```
Tier_3#sh run
ipv6 unicast-routing
!
interface FastEthernet0/0
 description To_ISP_B
 no ip address
 duplex auto
 speed auto
 ipv6 address 4151:5555::72F:67CC:FC55:F931/64
 ipv6 enable
!
interface FastEthernet2/1
 description To_ISP_Core
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:2222::21B:54FF:FE54:F112/64
 ipv6 enable
!
end
```

Elaborado por: Fausto Flores

Paso 3: Configuración de BGP – Multihoming. En la tabla 24 se realiza una descripción de los comandos utilizados para la configuración de BGP -4 en los equipos.

Tabla 24 Descripción de línea de comandos, configuración BGP-4

Comando	Descripción
Router(config)#**router bgp** id-AS	Para habilitar Border Gateway Protocol (BGP) para el modo de configuración del router IPv6, utilizar el comando en modo de configuración global.
Router(config-router)#**bgp router-id** x.x.x.x	El ID del router identifica de forma exclusiva un router dentro de un dominio OSPF. El comando se utiliza para definir de forma manual el identificador del router.
Router(config-router)#no **bgp default ipv4-unicast**	Desactiva la opción de unicast para IPv4.
Router(config-router)#**bgp log-neighbor-changes**	Muestra en consola si existe algún cambio dentro de la topología OSPF.
Router(config-router)#**neighbor** x.x.x.x.x.x.x:x remote-as id-AS	Agrega a un sistema autónomo a BGP, al especificar la IP y número de sistema autónomo remoto.
Router(config-router)# neighbor x.x.x.x.x.x.x:x ebgp-multihop 2	Es utilizado para indicar que existe más de un camino para llegar a un mismo destino.
Router(config-router)#address-family ipv6	Ingresa al modo de configuración específica correspondiente al protocolo IPv6.
Router(config-router-af)#neighbor x.x.x.x.x.x.x:x activate	Activa la sesión en el punto local, adicional la sesión también debe ser activada manualmente en el punto remoto.
Router(config-router-af)#neighbor x.x.x.x.x.x.x:x weight 1000	Se utiliza para la elección de la mejor ruta. La ruta con valor máximo de peso se considera como la mejor ruta.
Router(config-router-af)#network x.x.x.x.x.x.x:x /64	Hace referencia a la red que se encuentra dentro del sistema autónomo y que se desea publicar.
Router(config-router-af)#redistribute ospf 1	Anuncia a los prefijos aprendidos de forma dinámica, mediante el protocolo OSPF.
Router(config-router-af)#exit-address-family	Sale del modo de configuración específico para IPv6.

Elaborado por: Fausto Flores

Configuración BGP-4 Router Core:

Mediante el comando s*how run* se verifica la configuración de BGP-4 aplicada al router CORE.

Figura 51 Configuración BGP-4 Router Core

```
CORE#sh run
!
router bgp 100
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2001:ABCD::21B:54FF:FEA9:24B2 remote-as 200
 neighbor 2001:ABCD::21B:54FF:FEA9:24B2 ebgp-multihop 2
 neighbor 2002:ABCD::21B:54FF:FE54:FB12 remote-as 300
 neighbor 2002:ABCD::21B:54FF:FE54:FB12 ebgp-multihop 4
 neighbor 2001:2222::21B:54FF:FE54:F112 remote-as 400
 neighbor 2001:2222::21B:54FF:FE54:F112 ebgp-multihop 6
 !
 address-family ipv6
 neighbor 2001:ABCD::21B:54FF:FEA9:24B2 activate
 neighbor 2001:ABCD::21B:54FF:FEA9:24B2 weight 1000
 neighbor 2002:ABCD::21B:54FF:FE54:FB12 activate
 neighbor 2002:ABCD::21B:54FF:FE54:FB12 weight 250
 neighbor 2001:2222::21B:54FF:FE54:F112 activate
 neighbor 2001:2222::21B:54FF:FE54:F112 weight 500
 network 2001:DB8:0:1::/64
 network 2001:FBC:DA42:3::/64
 network 2002:ADB8:0:3::/64
 network 2003:AC9:0:4::/64
 network 2004:BF9:0:5::/64
 redistribute ospf 1
 no synchronization
 exit-address-family
!
end
```

Elaborado por: Fausto Flores

Configuración BGP-4 Router Tier_1:

Mediante el comando s*how run* se verifica la configuración de BGP-4 aplicada al router Tier_1.

Figura 52 Configuración BGP-4 Router Tier_1

```
Tier_1#sh run
!
router bgp 200
 bgp router-id 2.2.2.2
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2001:ABCD::21B:54FF:FEA9:24B1 remote-as 100
 neighbor 2001:ABCD::21B:54FF:FEA9:24B1 ebgp-multihop 2
 neighbor 8502:3333::21B:54AB:FE54:A212 remote-as 500
 !
 address-family ipv6
 neighbor 2001:ABCD::21B:54FF:FEA9:24B1 activate
 neighbor 2001:ABCD::21B:54FF:FEA9:24B1 weight 1000
 neighbor 8502:3333::21B:54AB:FE54:A212 activate
 network 2001:ABCD::/64
 network 8502:3333::/64
 exit-address-family
!
end
```

Elaborado por: Fausto Flores

Configuración BGP-4 Router Tier_2:

Mediante el comando s*how run* se verifica la configuración de BGP-4 aplicada al router Tier_2.

Figura 53 Configuración BGP-4 Router Tier_2

```
Tier_2#sh run
!
router bgp 300
 bgp router-id 3.3.3.3
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2002:ABCD::21B:54FF:FE54:FB11 remote-as 100
 neighbor 5602:5555::72A:65CC:CA55:A622 remote-as 700
 !
 address-family ipv4
 neighbor 2002:ABCD::21B:54FF:FE54:FB11 activate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv6
 neighbor 2002:ABCD::21B:54FF:FE54:FB11 activate
 neighbor 2002:ABCD::21B:54FF:FE54:FB11 default-originate
 neighbor 2002:ABCD::21B:54FF:FE54:FB11 weight 250
 neighbor 5602:5555::72A:65CC:CA55:A622 activate
 neighbor 5602:5555::72A:65CC:CA55:A622 default-originate
 network 5602:5555::/64
 exit-address-family
!
end
```

Elaborado por: Fausto Flores

Configuración BGP-4 Router Tier_3:

Mediante el comando s*how run* se verifica la configuración de BGP-4 aplicada al router Tier_3.

Figura 54 Configuración BGP-4 Router Tier_3

```
Tier_3#s run
!
router bgp 400
 no synchronization
 bgp router-id 4.4.4.4
 bgp log-neighbor-changes
 redistribute static
 neighbor 4151:5555::72F:67CC:FC55:F932 remote-as 700
 neighbor 2001:2222::21B:54FF:FE54:F111 remote-as 100
 no auto-summary
 address-family ipv6
 neighbor 4151:5555::72F:67CC:FC55:F932 activate
 neighbor 2001:2222::21B:54FF:FE54:F111 activate
 neighbor 2001:2222::21B:54FF:FE54:F111 weight 500
 network 4151:5555::/64
 exit-address-family
!
end
```

Elaborado por: Fausto Flores

Configuración de Path Attributes en BGP-4:

Tabla 25 Descripción de línea de comandos, configuración de path attributes

Comando	Descripción
Router(config)#router bgp AS	Para habilitar Border Gateway Protocol (BGP) para el modo de configuración del router IPv6, utilizar el comando en modo de configuración global.
Router(config-router)#neighbor ::/x next-hop-self	Establece como valor de next-hop la IP local
Router(config-router)#neighbor ::/x route-map local-pref in	Aplica la configuración de route map para el Path Attribute local-pref. Determina el mejor camino para el tráfico saliente, el valor por defecto es 100
Router(config-router)#neighbor ::/x weight 100	Este Path Attribute tiene un valor por defecto 0, el máximo valor de weight es considerado el mejor camino
CORE(config)#ipv6 prefix-list MATCH permit ::/0	El comando permite crear una lista que contenga prefijos IPv6.
CORE(config)#route-map local-pref permit 10	Permite configurar parámetros de ruteo, se puede utilizar con prefijos IPv4 e IPv6.
CORE(config-route-map)#match ip address prefix-list MATCH	Asigna las direcciones guardadas en la prefix-list llamada MATCH a Route map
CORE(config-route-map)#set local-preference número	Configura el valor del Path attribute loca-preference

Elaborado por: Fausto Flores

Mediante el comando show run en la figura 64 se verifica la configuración de los Path Attributes, aplicados al router CORE referente a BGP-4.

Figura 55 Configuración de Path Attributes

```
outer bgp 100
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2001:2222::21B:54FF:FE54:F112 remote-as 400
 neighbor 2001:2222::21B:54FF:FE54:F112 ebgp-multihop 6
 neighbor 2001:ABCD::21B:54FF:FEA9:24B2 remote-as 200
 neighbor 2001:ABCD::21B:54FF:FEA9:24B2 ebgp-multihop 2
 neighbor 2002:ABCD::21B:54FF:FE54:FB12 remote-as 300
 neighbor 2002:ABCD::21B:54FF:FE54:FB12 ebgp-multihop 4
 !
 address-family ipv6
 neighbor 2001:2222::21B:54FF:FE54:F112 activate
 neighbor 2001:2222::21B:54FF:FE54:F112 weight 500
 neighbor 2001:ABCD::21B:54FF:FEA9:24B2 activate
 neighbor 2001:ABCD::21B:54FF:FEA9:24B2 weight 1000
 neighbor 2001:ABCD::21B:54FF:FEA9:24B2 route-map local-pref in
 neighbor 2002:ABCD::21B:54FF:FE54:FB12 activate
 neighbor 2002:ABCD::21B:54FF:FE54:FB12 weight 250
 network 2001:AC9:0:4::/64
 network 2001:BF9:0:5::/64
 network 2001:DB8:0:1::/64
 network 2001:FBC:DA42:3::/64
 network 2002:ADB8:0:3::/64
 redistribute ospf 1
 no synchronization
 exit-address-family
!
!
no ip http server
no ip http secure-server
!
!
ipv6 router ospf 1
 router-id 3.3.4.3
 log-adjacency-changes
 redistribute connected
 redistribute static
 redistribute bgp 100
!
!
!
ipv6 prefix-list MATCH seq 5 permit 2001:ABCD::/64
ipv6 prefix-list MATCH seq 10 permit 2001:AC9:0:4::/64
ipv6 prefix-list MATCH seq 15 permit 2001:BF9:0:5::/64
ipv6 prefix-list MATCH seq 20 permit 2001:DB8:0:1::/64
ipv6 prefix-list MATCH seq 25 permit 2001:FBC:DA42:3::/64
ipv6 prefix-list MATCH seq 30 permit 2002:ADB8:0:3::/64
route-map local-pref permit 10
 match ipv6 address prefix-list MATCH
 set local-preference 1000
!
!
```

Elaborado por: Fausto Flores

.

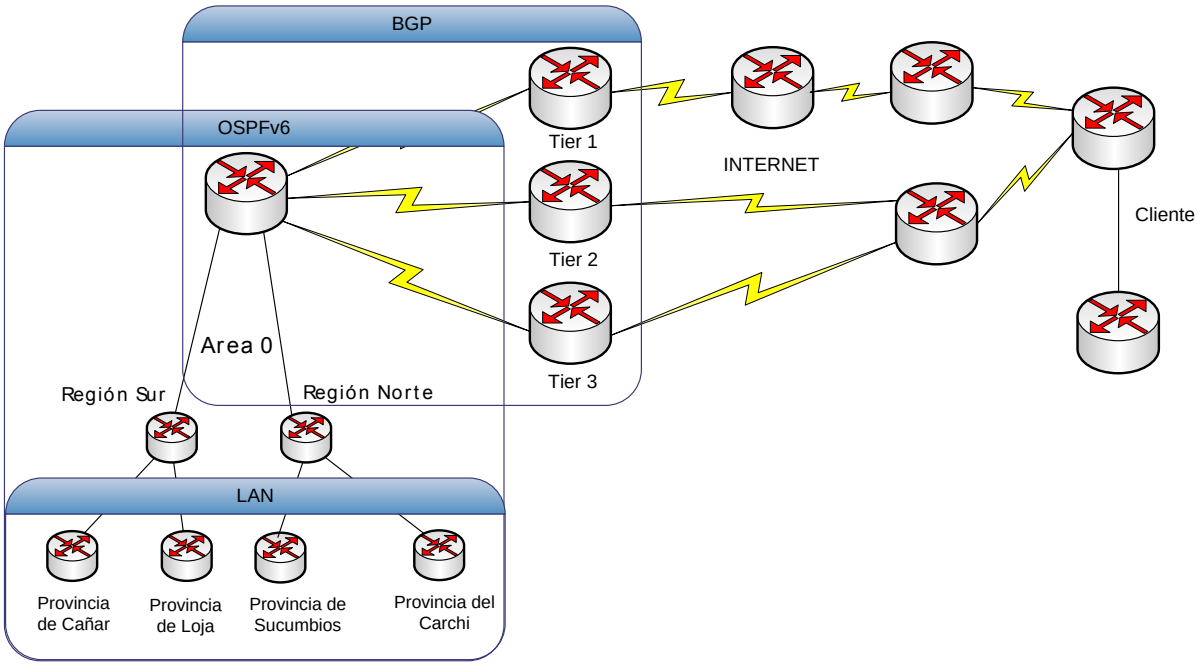
CAPÍTULO 4
EMULACIÓN

4.1 Escenarios de simulación

4.1.1 Descripción del escenario de simulación con Multihoming

En la figura 56 se describe el diagrama de red emulado, para el caso se tiene 3 salidas internacionales y el sistema autónomo se encuentra configurado con OSPFv3.

Figura 56 Diagrama de Red Multihomed

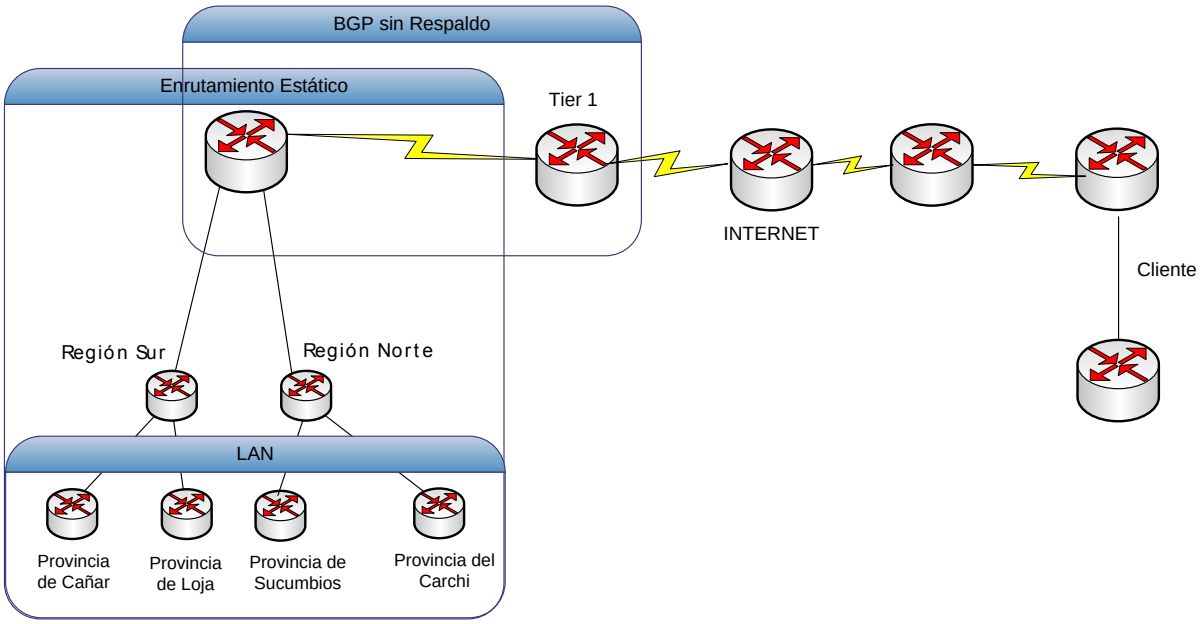


Elaborado por: Fausto Flores

4.1.2 Topología del escenario de simulación sin Multihoming

La figura 57 describe el diagrama de red sin respaldo en BGP y con enrutamiento estático.

Figura 57 Topología de red sin respaldo



Elaborado por: Fausto Flores

4.2 Pruebas y resultados: sistema autónomo y multihoming con ipv6

4.2.1 Pruebas y resultados: verificación de enrutamiento LAN

En la tabla 26 se realiza una comparativa de enrutamiento LAN entre un Proveedor de servicio que posee un enlace de respaldo y un ISP que no a nivel de enrutamiento LAN.

Tabla 26 Tipo de Enrutamiento a nivel del sistema autónomo

ISP con respaldo y OSPFv3	ISP con respaldo y OSPFv3
Loja#sh ipv6 route IPv6 Routing Table - 20 entries Codes: C - Connected, L - Local, S - Static, R - RIP, B – BGP U - Per-user Static route I1 - ISIS L1, I2 - ISIS L2, IA - ISIS inter-area, IS - ISIS summary O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 OE2 2001:ABCD::/64 [110/20] via FE80::C804:CFF:FE98:8, FastEthernet0/0 OE2 2001:ABC:FD53:4::/64 [110/1] via FE80::C804:CFF:FE98:8, FastEthernet0/0 O 2001:DB8:0:1::/64 [110/3] vía FE80::C804:CFF:FE98:8, FastEthernet0/0 O 2001:DB8:0:2::/64 [110/3] via FE80::C804:CFF:FE98:8, FastEthernet0/0 C 2001:FBC:DA42:3::/64 [0/0] vía ::, FastEthernet1/0 L 2001:FBC:DA42:3::1/128 [0/0] vía ::, FastEthernet1/0 O 2002:ADB8:0:3::/64 [110/2] via FE80::C804:CFF:FE98:8, FastEthernet0/0 C 2003:AC9:0:4::/64 [0/0] via ::, FastEthernet0/0 L 2003:AC9:0:4::2/128 [0/0] via ::, FastEthernet0/0 O 2004:BF9:0:5::/64 [110/4] via FE80::C804:CFF:FE98:8, FastEthernet0/0 OE2 2002:ABCD::/64 [110/20] via FE80::C804:CFF:FE98:8, FastEthernet0/0 OE2 4151:5555::/64 [110/1] via FE80::C804:CFF:FE98:8, FastEthernet0/0 OE2 2001:2222::/64 [110/20] via FE80::C804:CFF:FE98:8, FastEthernet0/0 L FE80::/10 [0/0] vía ::, Null0 L FF00::/8 [0/0] vía ::, Null0	Loja#sh ipv6 route IPv6 Routing Table - 7 entries Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP U - Per-user Static route I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 S ::/0 [1/0] vía 2003:AC9:0:4::1 C 2001:FBC:DA42:3::/64 [0/0] via ::, FastEthernet1/0 L 2001:FBC:DA42:3::1/128 [0/0] via ::, FastEthernet1/0 C 2003:AC9:0:4::/64 [0/0] via ::, FastEthernet0/0 L 2003:AC9:0:4::2/128 [0/0] via ::, FastEthernet0/0 L FE80::/10 [0/0] via ::, Null0 L FF00::/8 [0/0] vía ::, Null0

Elaborado por: Fausto Flores

Tabla 27 Comentarios tipo de Enrutamiento a nivel del sistema autónomo

Comentarios	Comentarios
• El algoritmo de Dijkstra es el encargado de determinar la ruta más corta hacia el destino. • El comando *show IPv6 route* despliega las rutas aprendidas. • El tiempo en que OSPFv6 tarda en catalogar el enlace del vecino como fuera de servicio es 39s. Mediante el comando show ipv6 ospf neighbor se puede verificar el tiempo de Dead Tme. • Al agregar una ruta o realizar un cambio en la red LAN, el protocolo OSPFv3 actualiza de manera automática la información en la tabla de enrutamiento.	• El router no conoce las redes de sus vecinos a menos que las rutas sean ingresadas de manera manual. • Si la red LAN posee una única salida, se configura una ruta por defecto, para el caso de IPv6 ::/0. • El uso de este tipo de enrutamiento es adecuado cuando se tiene una sola salida hacia las demás redes.

Elaborado por: Fausto Flores

Con el uso del comando show ipv6 ospf neighbor se puede verificar que el valor de dead time para un enlace activo tiene un valor de 39s, luego de presentarse una caída el contador decrece a 0s y el log de OSPFv6 muestra la pérdida de conexión. A continuación se detalla el proceso:

Figura 58 Enlace vecino activo

```
Loja# show ipv6 ospf neighbor
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.4.1           1   FULL/DR         00:00:39    4               FastEthernet0/0
```

Elaborado por: Fausto Flores

En la figura número 59 se puede verificar la pérdida del enlace mediante el comando show ipv6 ospf neighbor

Figura 59 Enlace vecino caído

```
show ipv6 ospf neighbor
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.4.1           1   FULL/DR         00:00:00    4               FastEthernet0/0
```

Elaborado por: Fausto Flores

En la fugura número 60 se puede verificar la pérdida del enlace vecino

Figura 60 Log donde se muestra pérdida de conexión con el vecino

```
*Dec 25 18:07:40.787: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.4.1 on FastEthernet0/0
from FULL to DOWN, Neighbor Down: Dead timer expired220 localhost.localdomain ESMTP
Sendmail 8.14.4/8.14.4;
```

Elaborado por: Fausto Flores

4.2.2 Verificación de enrutamiento OSPF

En la tabla 28 se realiza una comparativa de enrutamiento a nivel de un sistema autónomo con OSPF y un sistema autónomo con enrutamiento estático.

Tabla 28 Comparativa de enrutamiento a nivel de sistema autónomo

ISP con OSPF	ISP con enrutamiento estático
CORE#show ipv6 ospf neighbor Neighbor ID Pri State Dead Time Interface ID Interface 3.3.4.1 1 FULL/BDR 00:00:31 8 FastEthernet2/0 2.2.3.1 1 FULL/BDR 00:00:31 6 FastEthernet1/0	vía FE80::C804:CFF:FE98:8, S 2001:ABCD::/64 [110/20] via FE80::C804:1EFF:FE24:8, FastEthernet0/0 S 2001:DB8:0:1::/64 [110/3] via FE80::C804:1EFF:FE24:8, FastEthernet0/0 S 2001:DB8:0:2::/64 [110/3] via FE80::C804:1EFF:FE24:8, FastEthernet0/0 C 2001:FBC:DA42:3::/64 [0/0] vía ::, FastEthernet1/0 L 2001:FBC:DA42:3::1/128 [0/0] vía ::, FastEthernet1/0 S 2002:ADB8:0:3::/64 [110/2] via FE80::C804:1EFF:FE24:8, FastEthernet0/0 C 2003:AC9:0:4::/64 [0/0] via ::, FastEthernet0/0 L 2003:AC9:0:4::2/128 [0/0] via ::, FastEthernet0/0 S 2004:BF9:0:5::/64 [110/4] via FE80::C804:1EFF:FE24:8, FastEthernet0/0 S 2002:ABCD::/64 [110/20] via FE80::C804:1EFF:FE24:8, FastEthernet0/0 S 2001:2222::/64 [110/20] via FE80::C804:1EFF:FE24:8, FastEthernet0/0 L FE80::/10 [0/0] vía ::, Null0 L FF00::/8 [0/0] vía ::, Null0 Loja# L FE80::/10 [0/0]
Comentario	**Comentario**
• En la sesión OSPF el router de core presenta dos vecinos, el router concentrador Quito y el router concentrador Guayaquil. • Los routers dentro del dominio OSPFv3 tienen los siguientes estados DR (Designed Router) y BDR (Backup Designed Router). • El tiempo aproximado para propagar una ruta de 3 saltos es 4s. La base de datos DB (Data Base) es enviada desde el equipo en el que se generó el cambio hacia todos los vecinos.	• Cuando se realiza la configuración mediante ruteo estático y la red tiene un número elevado de equipos, la dificultad para la administración crece ya que cualquier cambio en la topología debe ser hecho de forma manual.

Elaborado por: Fausto Flores

En la figura 61 se puede verificar la pérdida de conexión, el log es presentado en el router de CORE, cuando el vecino MTZ_Guayaquil pierde conectividad.

Figura 61 Log de Pérdida de conexión OSPv6

```
*Dec 25 18:07:40.787: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.4.1 on FastEthernet0/0
from FULL to DOWN, Neighbor Down: Dead timer expired220 localhost.localdomain ESMTP
Sendmail 8.14.4/8.14.4;
```

Elaborado por: Fausto Flores

En la figura 62 se puede verificar que el vecino se recupera.

Figura 62 Log de adyacencia OSPFv6

```
*Dec 25 18:01:05.987: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.4.1 on FastEthernet0/0
from LOADING to FULL, Loading Done
```

Elaborado por: Fausto Flores

4.2.3 Verificación de enrutamiento BGP

En la tabla 29 se realiza una comparativa entre dos escenarios ISP, el primero con enlaces de respaldos en la salida internacional y el segundo escenario tiene una sola salida internacional.

Tabla 29 Comparativa de entre dos configuraciones ISP una con respaldo y otra sin respaldo

ISP con respaldo BGP	ISP sin respaldo BGP
CORE#show bgp ipv6 unicast summary BGP router identifier 1.1.1.1, local AS number 100 BGP table version is 84, main routing table version 84 15 network entries using 2235 bytes of memory 17 path entries using 1292 bytes of memory 17/11 BGP path/bestpath attribute entries using 2108 bytes of memory 12 BGP AS-PATH entries using 336 bytes of memory 0 BGP route-map cache entries using 0 bytes of memory 0 BGP filter-list cache entries using 0 bytes of memory BGP using 5971 total bytes of memory BGP activity 22/7 prefixes, 66/49 paths, scan interval 60 secs Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 2001:ABCD::21B:54FF:FEA9:24B2 4 200 159 157 84 0 0 00:00:41 8 2002:ABCD::21B:54FF:FE54:FB12 4 300 128 128 84 0 0 01:19:34 2 2001:2222::21B:54FF:FE54:F112 4 400 122 128 84 0 0 01:19:37 1	CORE#sh bgp ipv6 unicast summary BGP router identifier 1.1.1.1, local AS number 100 BGP table version is 10, main routing table version 10 7 network entries using 1043 bytes of memory 7 path entries using 532 bytes of memory 5/4 BGP path/bestpath attribute entries using 620 bytes of memory 3 BGP AS-PATH entries using 72 bytes of memory 0 BGP route-map cache entries using 0 bytes of memory 0 BGP filter-list cache entries using 0 bytes of memory BGP using 2267 total bytes of memory BGP activity 9/2 prefixes, 10/3 paths, scan interval 60 secs Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 2001:ABCD::21B:54FF:FEA9:24B2 4 200 12 12 10 0 0 00:03:48 5
Comentario	**Comentario**
• El comando show bgp ipv6 unicast summary, presenta 3 enlaces activos, uno principal y dos de respaldo.	• El comando show bgp ipv6 unicast summary, presenta 1 enlace activo sin respaldo. • Al no contar con un enlace de respaldo, el ISP este queda fuera de servicio.

Elaborado por: Fausto Flores

NOTA:

En la columna “ISP con respaldo BGP” referente a la tabla 29, se verifica los 3 enlaces de respaldo activo. En el caso de presentarse una caída, el comando *show bgp ipv6 unicast summary* permite verificar el estado del enlace, tal como se presenta en el siguiente ejemplo:

Figura 63 Estado de vecindades BGP-4

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:2222::21B:54FF:FE54:F112
                4   400      19      19       12    0    0 00:10:59        1
2001:ABCD::21B:54FF:FEA9:24B2
                4   200      14      21        0    0    0 00:02:56 Active
2002:ABCD::21B:54FF:FE54:FB12
                4   300      21      20       12    0    0 00:10:59        2
```

Elaborado por: Fausto Flores

4.2.4 Pruebas de conectividad desde la provincia de Loja hasta El Cliente

En la tabla 30 se realiza una prueba de ping con el fin de verificar la conectividad desde la provincia de Loja hasta un cliente que se encuentra fuera del ISP.

Tabla 30 Pruebas de conectividad a nivel de ISP

ISP con respaldo BGP	ISP sin respaldo BGP
Loja#ping 6473:8888::15C:78DD:CD88:C962 repeat 500 size 1500 Type escape sequence to abort. Sending 500, 100-byte ICMP Echos to 6473:8888::15C:78DD:CD88:C962, timeout is 2 seconds: !! !! !! !! !! !! !! !! !!!!!!!!!!!!!!!!!!! !! !!!!!!!!!!!!!!! Success rate is 100 percent (500/500), round-trip min/avg/max = 52/134/900 ms	Loja#ping 6473:8888::15C:78DD:CD88:C962 repeat 500 size 1500 Type escape sequence to abort. Sending 500, 100-byte ICMP Echos to 6473:8888::15C:78DD:CD88:C962, timeout is 2 seconds: !!! !!! !!! !!! !!! !!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!! Success rate is 100 percent (500/500), round-trip min/avg/max = 76/188/1996 ms
Comentario	**Comentario**
El total de saltos desde la provincia de Loja hasta el cliente son 5, con Multihomig BGP se descubre el camino más corto para llegar al destino. Para este caso el tiempo en que se tarda en completar la prueba es aproximadamente 134 ms. Tomando en cuenta 5 saltos.	El total de saltos para llegar al destino es 6. BGP solo tiene un camino para llegar al destino. El tiempo que tarda en completarse es la prueba es aproximadamente 188 ms. Tomando en cuenta 6 saltos

Elaborado por: Fausto Flores

4.2.5 Pruebas de conectividad BGP

En la tabla 31 se realiza una prueba de ping con el fin de verificar la conectividad a través de BGP desde la provincia de Loja hasta un cliente que se encuentra fuera del

ISP. El objetivo es verificar el buen funcionamiento del enlace de respaldo. Para esta prueba el enlace principal se encuentra fuera de servicio.

Tabla 31 Comparativa de BGP Multihoming

ISP con respaldo BGP	ISP sin respaldo BGP
Loja#ping 6473:8888::15C:78DD:CD88:C962 repeat 1500 size 1500 Type escape sequence to abort. Sending 1500, 100-byte ICMP Echos to 6473:8888::15C:78DD:CD88:C962, timeout is 2 seconds: !!!............ ....!!!!! !!! !!! !!! !!! !!! !!! !!! !!! !!! !!! !!! Success rate is 94 percent (1419/1500), round-trip min/avg/max = 36/107/348 ms	Loja#ping 6473:8888::15C:78DD:CD88:C962 repeat 1500 size 1500 Type escape sequence to abort. Sending 1500, 100-byte ICMP Echos to 6473:8888::15C:78DD:CD88:C962, timeout is 2 seconds: !!............. .... Success rate is 3 percent (55/1500), round-trip min/avg/max = 44/104/176 ms
Comentario	**Comentario**
Paquetes recibidos 94%, al presentarse una caída en el enlace de respaldo, el enlace secundario entra en funcionamiento. Los paquetes perdidos suman 81 durante la transición de enlace.	Pérdida total en la conexión. Cuando el enlace principal sufre una caída, el ISP queda fuera de servicio.

Elaborado por: Fausto Flores

4.2.5.1 Traceroute con el enlace principal activo

En la tabla 32 se realiza una traza con el fin de verificar la ruta que toman los paquetes, desde la provincia de Loja hasta el cliente que se encuentra fuera del ISP.

Tabla 32 Comparativa de saltos desde el cliente hasta el servidor

ISP con respaldo BGP	ISP sin respaldo BGP
Loja#traceroute 6473:8888::15C:78DD:CD88:C962 Type escape sequence to abort. Tracing the route to 6473:8888::15C:78DD:CD88:C962 1 2003:AC9:0:4::1 12 msec 28 msec 28 msec 2 2002:ADB8:0:3::1 48 msec 8 msec 52 msec 3 2001:2222::21B:54FF:FE54:F112 24 msec 76 msec 68 msec 4 4151:5555::72F:67CC:FC55:F932 108 msec 48 msec 44 msec 5 5262:7777::94B:89EE:BC77:B252 68 msec 68 msec 80 msec 6 6473:8888::15C:78DD:CD88:C962 168 msec 140 msec 96 msec	Loja#traceroute 2001:ABC:FD53:4::1 Type escape sequence to abort. Tracing the route to 2001:ABC:FD53:4::1 1 2003:AC9:0:4::1 44 msec 24 msec 12 msec 2 2002:ADB8:0:3::1 52 msec 40 msec 28 msec 3 2001:ABCD::21B:54FF:FEA9:24B2 80 msec 28 msec 24 msec 4 8502:3333::21B:54AB:FE54:A212 76 msec 72 msec 44 msec 5 7601:4444::32C:64BB:FA44:C522 96 msec 100 msec 88 msec 6 3742:6666::83A:78DD:AB66:A142 108 msec 92 msec 120 msec 7 2001:ABC:FD53:4::1 88 msec 92 msec 128 msec
Comentario	**Comentario**
• La traza se completa de manera satisfactoria, con un total de 6 saltos. • La configuración de Multihoming BGP escoge la mejor ruta, con lo cual se alcanza el destino con el camino más corto.	• La traza se completa de manera satisfactoria, con un total de 7 saltos. • BGP dispone de una sola salida internacional.

Elaborado por: Fausto Flores

4.2.5.2 Traceroute con el enlace principal fuera de servicio

En la tabla 33 se realiza una traza con el fin de verificar la ruta que toman los paquetes, desde la provincia de Loja hasta el cliente que se encuentra fuera del ISP, para este caso el enlace principal se encuentra fuera de servicio.

Tabla 33 Comparativa de saltos desde el cliente hasta el servidor con Multihoming

ISP con respaldo BGP	ISP sin respaldo BGP
Tracing the route to 2001:ABC:FD53:4::1 1 2003:AC9:0:4::1 152 msec 28 msec 100 msec 2 2001:2222::21B:54FF:FE54:F112 72 msec 56 msec 60 msec 3 4151:5555::72F:67CC:FC55:F932 56 msec 80 msec 52 msec 4 5262:7777::94B:89EE:BC77:B252 120 msec 60 msec 80 msec 5 2001:ABC:FD53:4::1 152 msec 104 msec 100 msec	Loja#traceroute 2001:ABC:FD53:4::1 Type escape sequence to abort. Tracing the route to 2001:ABC:FD53:4::1 1 2003:AC9:0:4::1 24 msec 16 msec 16 msec 2 2002:ADB8:0:3::1 24 msec 32 msec 36 msec 3 * * * 4 * * * 5 * * * 6 * * * 7 * * * 8 * * * 9 * * * 10 * * * 11 * * * 12 * * * 13 * * *
Comentario	**Comentario**
• Como se puede observar en el salto número 2 la ruta del enlace principal ha sido reemplazada por la del enlace de respaldo. • Al presentarse una caída en el enlace principal el enlace de respaldo entra a funcionar.	• Al presentarse una caída en el enlace WAN, se pierde la conectividad y el comando traceroute muestra desde el tercer salto pérdida de conexión.

Elaborado por: Fausto Flores

En la figura 64 se puede verificar la caída del enlace principal, cuando se presenta la caída el enlace pasa al estado de ACTIVO

Figura 64 Log de pérdida de conexión BGP-4

```
*Dec 25 19:04:23.187: %BGP-3-NOTIFICATION: sent to neighbor
2001:ABCD::21B:54FF:FEA9:24B2 4/0 (hold time expired) 0 bytes
```

Elaborado por: Fausto Flores

En la figura 65 se puede verificar que el enlace principal se recupera.

Figura 65 Log adyacencia BGP-4

```
*Dec 25 19:07:31.427: %BGP-5-ADJCHANGE: neighbor 2001:ABCD::21B:54FF:FEA9:24B2 Up
```

Elaborado por: Fausto Flores

4.3 Pruebas y resultados servidores ftp, http y smtp con ipv6

En esta sección se verifica el funcionamiento de los servidores FTP, HTTP y SMTP.

4.3.1 Pruebas en el servidor FTP sobre IPv6

Para las pruebas de FTP se utilizará un escenario cliente-servidor, en el cual un cliente ubicado fuera del ISP realiza cargas y descargas de archivos hacia el servidor.

Adicional, para probar el funcionamiento, mediante telnet se verifica la conectividad al puerto 21.

4.3.1.1 Prueba de conectividad al puerto 21

Mediante el uso de telnet, se verifica que el puerto 21 FTP se encuentra activo. La siguiente respuesta de consola, indica que la conexión ha sido exitosa.

Figura 66 Diagrama de Red Multihomed

```
[root@localhost ~]# telnet  2001:fbc:da42:3::2 21
Trying 2001:fbc:da42:3::2...
Connected to 2001:fbc:da42:3::2.
Escape character is '^]'.
220 BIENVENIDO.
```

Elaborado por: Fausto Flores

4.3.1.2 Autenticación al servidor

Mediante el uso de comando FTP en modo consola, se realiza la petición al servidor manera remota, una vez aceptada la conexión se procede a la autenticación en el sistema para el caso se utiliza el siguiente usuario y contraseña:

Usuario: test

Contraseña: 26532162

Figura 67 Diagrama de Red Multihomed

```
[root@localhost ~]# ftp 2001:fbc:da42:3::2
Connected to 2001:fbc:da42:3::2 (2001:fbc:da42:3::2).
220 BIENVENIDO.
Name (2001:fbc:da42:3::2:fausto): test
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||57723|).
150 Here comes the directory listing.
-rw-rw-r--    1 500      500            10 Sep 02 13:43 documento
226 Directory send OK.
ftp>
```

Elaborado por: Fausto Flores

4.3.1.3 Transferencia de archivos al servidor FTP

Carga

A través del cliente se envía un archivo al servidor FTP por medio del cliente remoto. Como se puede observar el nombre del documento es *Documento Prueba Subir*, la transferencia se realiza de manera exitosa.

Figura 68 Diagrama de Red Multihomed

```
[rene@localhost Desktop]$ ftp 2001:fbc:da42:3::2
Connected to 2001:fbc:da42:3::2 (2001:fbc:da42:3::2).
220 BIENVENIDO.
Name (2001:fbc:da42:3::2:rene): test
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put DocumentoPruebaSubir
local: DocumentoPruebaSubir remote: DocumentoPruebaSubir
229 Entering Extended Passive Mode (|||63900|).
150 Ok to send data.
226 Transfer complete.
ftp>
```

Elaborado por: Fausto Flores

Descarga

A través del cliente se descarga un archivo del servidor FTP por medio del cliente remoto. Como se puede observar el nombre del documento es *Documento Prueba Descarga*, la transferencia se realiza de manera exitosa.

Figura 69 Diagrama de Red Multihomed

```
Connected to 2001:fbc:da42:3::2 (2001:fbc:da42:3::2).
220 BIENVENIDO.
Name (2001:fbc:da42:3::2:rene): test
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||17507|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0               0 Nov 04 12:40 DocumentoPruebaDescarga
-rw-rw-r--    1 500      500            10 Sep 02 13:43 documento
drwxr-xr-x    2 0        0            4096 Nov 04 12:42 ps
226 Directory send OK.
ftp> get DocumentoPruebaDescarga
local: DocumentoPruebaDescarga remote: DocumentoPruebaDescarga
229 Entering Extended Passive Mode (|||18950|).
150 Opening BINARY mode data connection for DocumentoPruebaDescarga (0 bytes).
226 Transfer complete.
ftp>
```

Elaborado por: Fausto Flores

4.3.1.4 Logs de FTP

En la ruta /var/log/xferlog se encuentra el archivo de logs del servidor Very Secure FTP, en esta ruta el administrador de red puede verificar las peticiones de los usuarios al puerto 21.

Figura 70 Diagrama de Red Multihomed

```
Mon Nov  4 04:54:22 2013 1 2001:abc:fd53:4::2 0 /home/rene/DocumentoParaSubir b
_ i r test ftp 0 * i
Mon Nov  4 04:55:27 2013 1 2001:abc:fd53:4::2 0 /DocumentoPruebaDescarga b _ o r
 test ftp 0 * c
Mon Nov  4 04:58:20 2013 1 2001:abc:fd53:4::2 0 /DocumentoPruebaSubir b _ i r te
st ftp 0 * c
```

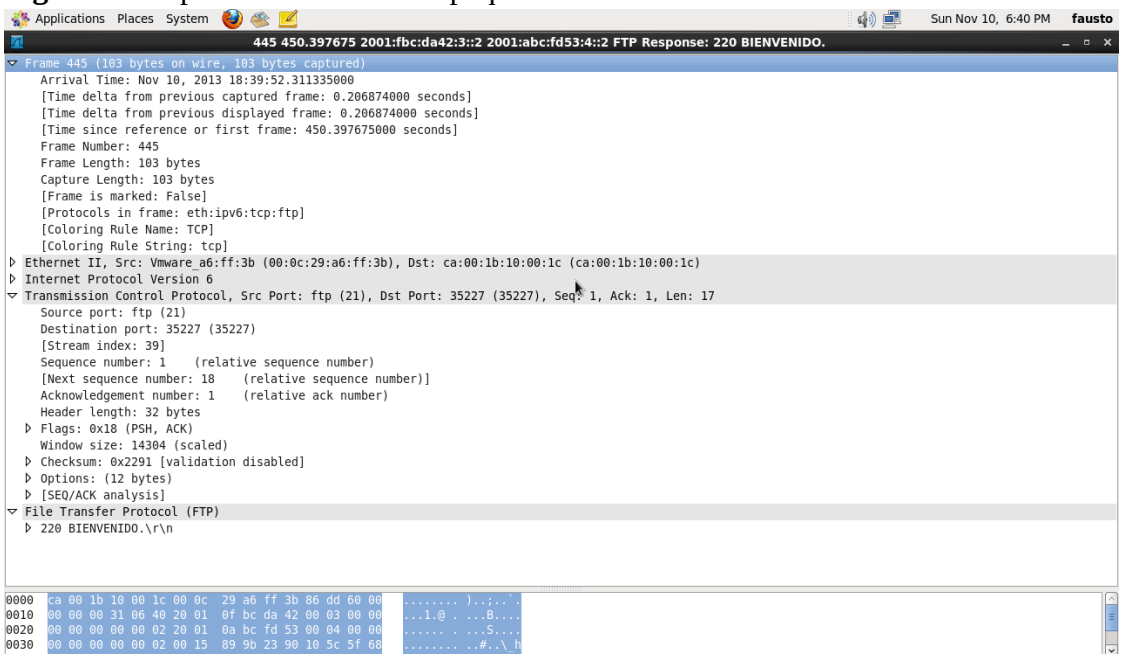
Elaborado por: Fausto Flores

Dentro del archivo de logs para FTP, como se puede verificar en la figura 70 desde el cliente remote se ha realizado la carga de un archivo “0 * c” y la descarga de otro “0 * i”.

4.3.1.5 Captura de paquetes con Wireshark sobre el puerto 21 FTP

Con el uso de la herramienta Wireshark se ha capturado el paquete dirigido hacia el puerto 21. En la figura 71 se observa el mensaje de bienvenida del servidor FTP.

Figura 71 Captura con Wireshark paquete FTP



Elaborado por: Fausto Flores

4.3.2 Pruebas del servidor HTTP sobre IPv6

4.3.2.1 Telnet al puerto 80

Mediante el uso de telnet, se verifica desde el cliente que la petición al puerto 80 HTTP, como se puede verificar en la salida que se presenta a continuación la conexión ha sido exitosa.

Figura 72 Telnet puerto 80

```
[rene@localhost Desktop]$ telnet 2001:fbc:da42:3::2 80
Trying 2001:fbc:da42:3::2...
Connected to 2001:fbc:da42:3::2.
Escape character is '^]'.
```

Elaborado por: Fausto Flores

4.3.2.2 Consulta de página web

Desde el cliente, se realiza la petición al puerto 80 por medio del navegador Mozilla Firefox. La página web se encuentra ubicada en el directorio /var/www/html/test.

Figura 73 Consulta de página WEB desde el cliente

Elaborado por: Fausto Flores

4.3.2.3 Logs de HTTP

En la ruta /var/log/httpd/access_log se encuentra el archivo de logs del servidor HTTP, en esta ruta el administrador de red puede verificar las peticiones de los usuarios correspondientes al puerto 80.

Figura 74 Consulta de página WEB desde el cliente

```
root@localhost httpd]# more access_log
2001:abc:fd53:4::2 - - [05/Nov/2013:19:12:01 -0800] "GET /prueba HTTP/1.1" 304 -
 "-" "Mozilla/5.0 (X11; Linux i686; rv:10.0.12) Gecko/20130109 Firefox/10.0.12"
```

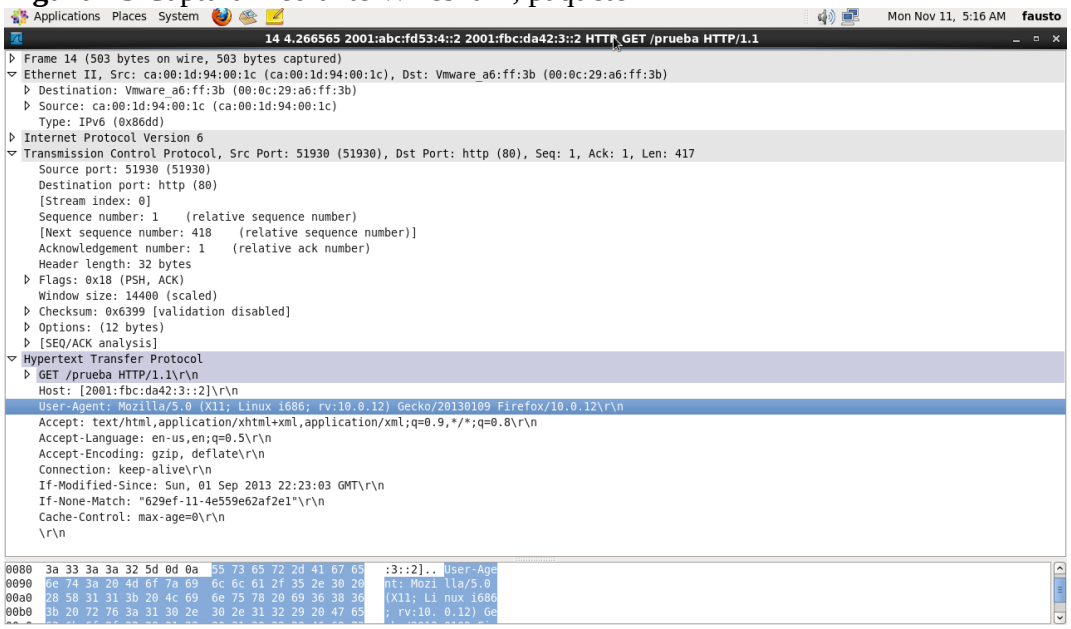
Elaborado por: Fausto Flores

Dentro del archivo de logs para HTTP como se puede verificar en la figura 83, se realizó una visita a la página WEB "GET /prueba HTTP/1.1" desde la IP "2001:abc:fd53:4::2", en la fecha "05/Nov/2013:19:12:01 -0800" y por medio del navegador "Mozilla/5.0 (X11; Linux i686; rv:10.0.12) Gecko/20130109 Firefox/10.0.12".

4.3.2.4 Captura de paquetes con Wireshark al puerto 80 HTTP

Con el uso de la herramienta Wireshark se ha capturado el paquete dirigido hacia el puerto 80. En la figura 30 se observa el mensaje de respuesta con la petición de la página web que tiene como nombre prueba.

Figura 75 Captura mediante Wireshark, paquete HTTP



Elaborado por: Fausto Flores

4.3.3 Pruebas de los servidores SMTP/POP3 sobre IPv6

4.3.3.1 Telnet al puerto 25/110

- **Telnet al puerto 25 SMTP**

Mediante el uso de telnet, se verifica que el puerto 25 SMTP se encuentra activo. La siguiente respuesta de consola, indica que la conexión ha sido exitosa.

Figura 76 Telnet puerto 25

```
 [root@localhost ~]# telnet 2001:fbc:da42:3::2 25
Trying 2001:fbc:da42:3::2...
Connected to 2001:fbc:da42:3::2.
Escape character is '^]'.
220 localhost.localdomain ESMTP Sendmail 8.14.4/8.14.4; Sun, 10 Nov 2013 07:38:05 -
0800
```

Elaborado por: Fausto Flores

- **Telnet al Puerto 110 POP3**

Mediante el uso de telnet, se verifica que el puerto 110 POP3 se encuentra activo. La siguiente respuesta de consola, indica que la conexión ha sido exitosa.

Figura 77 Telnet puerto 110

```
 [root@localhost ~]# telnet 2001:fbc:da42:3::2 110
Trying 2001:fbc:da42:3::2...
Connected to 2001:fbc:da42:3::2.
Escape character is '^]'.
+OK Dovecot ready.
```

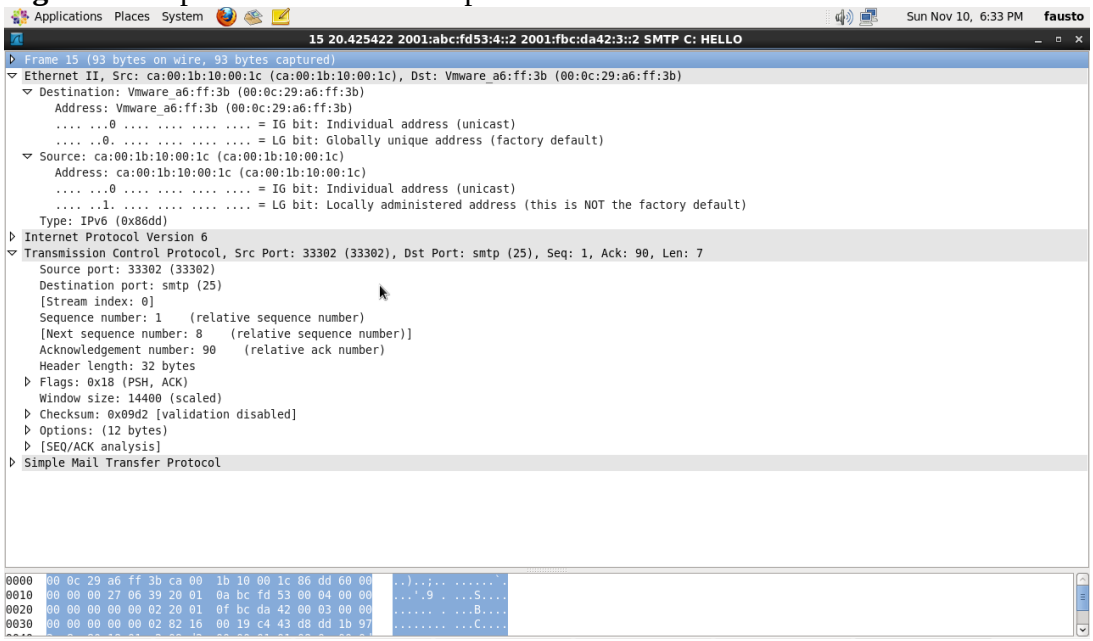
Elaborado por: Fausto Flores

4.3.3.2 Captura de paquetes con Wireshark a los puertos 25/110 SMTP/POP

- **Captura de paquetes con el uso de Wireshark al puerto 25 SMTP**

Con el uso de la herramienta Wireshark se ha capturado el paquete dirigido hacia el puerto 25. En la figura 87 se observa el mensaje luego de establecer la conexión 25.

Figura 78 Captura de Wireshark al puerto 25



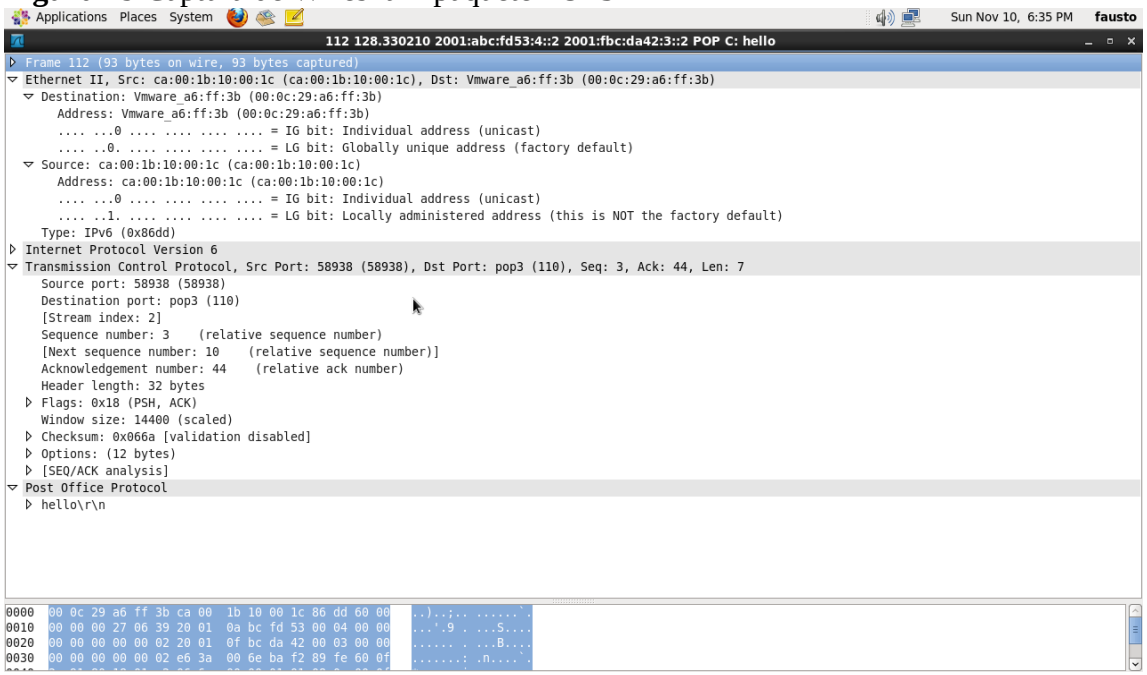
Elaborado por: Fausto Flores

- **Uso de Wireshark al puerto 110 POP3**

Con el uso de la herramienta Wireshark se ha capturado el paquete dirigido hacia el puerto 110.

En la figura 79 se observa el mensaje luego de establecer la conexión al puerto 110.

Figura 79 Captura de Wireshark paquete POP3



Elaborado por: Fausto Flores

4.3.3.3 Envío y recepción de un correo electrónico

- **Envío de un correo electrónico**

En la siguiente salida de consola se observa el envío de correo con el uso del comando mail.

Figura 80 Captura de Wireshark paquete POP3

```
 [root@localhost ~]# mail rene
Subject: prueba
hola.
.
EOT
[root@localhost ~]#
You have mail in /var/spool/mail/root
```

Elaborado por: Fausto Flores

- **Recepción de un correo electrónico**

Los buzones de los usuarios se encuentran en la ruta /var/mail/, para este caso se consultara el buzón de entrada del usuario rene en la siguiente ruta /var/mail/rene

Figura 81 Captura de Wireshark paquete POP3

```
rom fausto@localhost.localdomain  Sun Nov 10 07:57:00 2013
Return-Path: <fausto@localhost.localdomain>
Received: from localhost.localdomain (localhost [127.0.0.1])
         by localhost.localdomain (8.14.4/8.14.4) with ESMTP id rAAFv0Ht008325
         for <rene@localhost.localdomain>; Sun, 10 Nov 2013 07:57:00 -0800
Received: (from root@localhost)
         by localhost.localdomain (8.14.4/8.14.4/Submit) id rAAFv0hn008324
         for rene; Sun, 10 Nov 2013 07:57:00 -0800
From: fausto <fausto@localhost.localdomain>
Message-Id: <201311101557.rAAFv0hn008324@localhost.localdomain>
Date: Sun, 10 Nov 2013 07:57:00 -0800
To: rene@localhost.localdomain
Subject: prueba
User-Agent: Heirloom mailx 12.4 7/29/08
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

hola.
```

Elaborado por: Fausto Flores

4.3.3.4 Logs de SMTP/POP3

En la ruta /var/log/maillog se encuentra el archivo de logs del servidor SMTP, en esta ruta el administrador de red puede verificar las peticiones el uso del servidor con respecto al puerto 25/110.

Figura 82 Captura de Wireshark paquete POP3

```
Nov 10 07:57:00 localhost sendmail[8324]: rAAFv0hn008324: from=fausto, size=203,
class=0, nrcpts=1, msgid=<201311101557.rAAFv0hn008324@localhost.localdomain>,
relay=root@localhost
Nov 10 07:57:00 localhost sendmail[8325]: rAAFv0Ht008325:
from=<fausto@localhost.localdomain>, size=475, class=0, nrcpts=1,
msgid=<201311101557.rAAFv0hn008324@localhost.localdomain>, proto=ESMTP, daemon=MTA,
relay=localhost [127.0.0.1]
Nov 10 07:57:00 localhost sendmail[8324]: rAAFv0hn008324: to=rene, ctladdr=fausto
(500/500), delay=00:00:00, xdelay=00:00:00, mailer=relay, pri=30203,
relay=[127.0.0.1] [127.0.0.1], dsn=2.0.0, stat=Sent (rAAFv0Ht008325 Message
accepted for delivery)
Nov 10 07:57:00 localhost sendmail[8326]: rAAFv0Ht008325:
to=<rene@localhost.localdomain>, ctladdr=<fausto@localhost.localdomain> (500/500),
delay=00:00:00, xdelay=00:00:00, mailer=local, pri=30698, dsn=2.0.0, stat=Sent
```

Elaborado por: Fausto Flores

Dentro del archivo de logs, en la figura 91 se verifica que el mensaje se ha enviado de manera satisfactoria con el mensaje “stat=Sent” así también el demonio que se utilizó para la transferencia “daemon=MTA”. El usuario que envió el correo “from=fausto” el cual es un usuario local,”msgid=<201311101557.rAAFv0hn008324@localhost.localdomain>” y hacia que cuenta fue enviado “to=<rene@localhost.localdomain>”.

CONCLUSIONES

✓ Se ha finalizado con éxito el proyecto de grado y de manera satisfactoria, con el estudio se ha podido verificar que las configuraciones, análisis y emulación es viable, así también su implementación si en un futuro se lo desea realizar en un escenario real.

✓ La topología emulada consta de 3 escenarios: Red LAN, Sistema autónomo del ISP y la conexión de BGP con Multihoming. Con esta división la administración de la red y manejo de troubleshootings se puede solucionar de una manera rápida y eficaz sin que todo el ISP se vea afectado.

✓ La emulación de una red Multihoming es posible gracias al protocolo BGP-4 y a la manipulación de sus Path Attributes. Es factible combinar varios Path Attributes para el que resultado se acople a los requerimientos de cada red en particular, con lo cual se obtiene una solución efectiva para cada uno de los distintos escenarios.

✓ El uso de OSPFv3 dentro del sistema autónomo es óptimo para escenarios en los que se requiere escalabilidad, su habilidad para reaccionar y adaptarse sin perder calidad en la red es propia del protocolo y con el uso de IPv6 se aporta mayor seguridad a la red ya que dentro de sus características se incluye compatibilidad con IPSec.

✓ El protocolo OSPFv3 se adapta de mejor manera a las redes jerárquicas ya que dentro de cada área se puede definir el tipo de información y rutas que se va propagar a sus vecinos, para la salida y entrada de información del Sistema Autónomo.

✓ Las configuraciones y las políticas que se aplican para BGP-4 y el manejo del tráfico entrante y saliente, pueden ser aplicadas de manera independiente, con lo cual el manejo de datos se puede personalizar a cada escenario.

✓ Al realizar la emulación de multihoming con IPv6, se pudo observar que por default BGP escoge la ruta con menor cantidad de Sistemas Autónomos para llegar al destino, si se desea cambiar el camino la manipulación de Path Attributes es obligatorio para obtener los resultados de acuerdo a las necesidades de cada escenario.

✓ Las interfaces de los programas GNS3 y VMWare son amigables con el usuario y permiten acceder a las funcionalidades y características que los equipos reales poseen. Sin invertir grandes cantidades de dinero permitiendo planificar escenarios de pruebas para un posterior desarrollo e implementación.

✓ Con la virtualización y consolidación de los servidores WEB, FTP y servidor de Correo a través de VMWare se logra reducir costos en la adquisición de equipamiento físico, ahorro de energía en equipos de climatización y reducción de espacio en data centers. Adicional, brinda una mejor gestión de recursos como tiempo y dinero sin sacrificar el rendimiento de los servidores.

RECOMENDACIONES

✓ Si se desea ampliar el estudio de grado se recomienda emular o implementar un Servidor de Nombres de dominio DNS orientado a IPv6 con el fin de obtener una resolución de IPv6 a nivel de los clientes.

✓ Para la sección de BGP–Multihomig se recomienda mantener la configuración por defecto del tiempo en que BGP-4 tarda en bloquear y desbloquear la vecindad. En el caso de presentar intermitencias un enlace BGP-4 el ISP puede ser penalizado, ya que anuncia y retira prefijos ocasionando que las tablas de rutas del internet se actualicen cada vez que se produce un cambio en el estado del enlace.

✓ Para la configuración de los Path Attributes de BGP-multihoming se debe evaluar las necesidades de la red, con el fin de escoger las configuraciones que se adapten a las necesidades del Sistema Autónomo. Para que ciertos Path Attributes tengan efecto se debe contar con la colaboración del proveedor de servicios WAN.

✓ Para la ampliación del estudio se recomienda activar el protocolo SNMPv3 (Simple Network Management Protocol versión 3) en todos los equipos de la red y centralizar el monitoreo de logs, con la configuración de un servidor como LogAnalyzer y un servidor Nagios para mantener el monitoreo de las direcciones IPv6.

✓ Para la sección correspondiente a servidores, se recomienda ampliar el estudio con la emulación o implementación de arreglos RAID ya que el caso de presentarse un daño físico o lógico en el sistema operativo, los discos de respaldo entrarían a funcionar.

✓ Como alcance al proyecto se recomienda la instalación del servidor Smokeping cuya funcionalidad permite medir la pérdida de paquetes y latencia en la red así como obtener estadísticas mensuales de rendimiento, con esto se lograría evaluar el comportamiento de las salidas internacionales.

- ✓ Para la elección del protocolo IGP a utilizarse dentro del sistema autónomo, el administrador de red debe evaluar los requerimientos de la red, costo de equipamiento, tanto para el core como para el cliente final.

- ✓ Como alcance al proyecto, para la topología se recomienda incluir el uso de Route Reflectors (RR) ya que enseñan las rutas a los demás equipos de la red y al mismo tiempo reduce la carga de procesamiento.

- ✓ En el uso de BGP, se recomienda que para la configuración de un AS Multihomed este AS, no funcione como Sistema Autónomo (AS) de tránsito para el tráfico que proviene de Internet, de manera que toda la información que viaje por el AS sea local. Para ello, no se debe anunciar hacia el exterior ninguna ruta que no tenga origen en este AS, ya que anunciar una ruta implica aceptar todo el tráfico que tenga como destino esa ruta.

LISTA DE REFERENCIAS

- ✓ *CISCO*. (2011). Recuperado el 29 de octubre de 2013, de www.cisco.com/en/US/docs/security/asdm/6_1/user/guide/routing.html#wp1090636

- ✓ *CISCO*. (2012). Recuperado el 29 de octubre de 2013, de www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/unicast/configuration/guide/l3_route.html

- ✓ *CISCO*. (2012). Recuperado el 27 de octubre de 2013, de www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a3e6f.shtml

- ✓ *ApacheOrg*. (2013). Recuperado el 23 de septiembre de 2013, de httpd.apache.org/docs/2.0/es/bind.html

- ✓ Barrios, J. (2009). *Alcance libre*. Recuperado el 12 de octubre de 2013, de www.alcancelibre.org/staticpages/index.php/introduccion-ipv4

- ✓ BSD, O. (2013). *Open SSH*. Recuperado el 14 de Septiembre de 2013, de www.openssh.com

- ✓ Cicileo, G., Gagliano, R., Flaherty, C., Olvera, C., Palet, J., Rocha, M., y otros. (2009). *IPv6 para todos Guía para uso y aplicaciçon para diversos entornos.* Buenos Aires.

- ✓ Hat, R. (2005). *Red Hat Enterprise Linux 4: Manual de referencia*. Recuperado el 12 de Septiembre de 2013, de web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-ftp-vsftpd-conf.html

✓ Hochman, E. (1978). *Técnicas de investigación documental.* Estados Unidos: Trillas.

✓ Millan, R. (2006). *Consultoria estratégica en tecnologías de la información y la comunicación* . Recuperado el 13 de agosto de 2013, de www.ramonmillan.com/tutoriales/ipv6_parte1.php

✓ Murphy, R., & Malone, D. (2005). *IPv6 Network Administration.* USA: O`reilly.

✓ Tamayo, M. (2004). *El proceso de la investigación científica.* México: Limusa.

✓ Van Beijnum, I. (2002). *BGP.* USA: O`reilly.